
April 30, 2005



Information Technology Management

Report on Standard Finance System Controls
Placed in Operation and Tests of Operating
Effectiveness for the Period October 1, 2004
through March 31, 2005 (D-2005-059)

Department of Defense
Office of the Inspector General

Constitution of
the United States

A Regular Statement of Account of the Receipts and Expenditures of all public
Money shall be published from time to time.

Article I, Section 9

Report Documentation Page				Form Approved OMB No. 0704-0188	
Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.					
1. REPORT DATE 30 APR 2005		2. REPORT TYPE N/A		3. DATES COVERED -	
4. TITLE AND SUBTITLE Information Technology Management: Report on Standard Finance System Controls Placed in Operation and Tests of Operating Effectiveness for the Period October 1, 2004 through March 31, 2005				5a. CONTRACT NUMBER	
				5b. GRANT NUMBER	
				5c. PROGRAM ELEMENT NUMBER	
6. AUTHOR(S)				5d. PROJECT NUMBER	
				5e. TASK NUMBER	
				5f. WORK UNIT NUMBER	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Inspector General Department of Defense 400 Army Navy Drive Arlington, VA 22202-4704				8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)				10. SPONSOR/MONITOR'S ACRONYM(S)	
				11. SPONSOR/MONITOR'S REPORT NUMBER(S)	
12. DISTRIBUTION/AVAILABILITY STATEMENT Approved for public release, distribution unlimited					
13. SUPPLEMENTARY NOTES The original document contains color images.					
14. ABSTRACT					
15. SUBJECT TERMS					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT UU	18. NUMBER OF PAGES 136	19a. NAME OF RESPONSIBLE PERSON
a. REPORT unclassified	b. ABSTRACT unclassified	c. THIS PAGE unclassified			



INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
400 ARMY NAVY DRIVE
ARLINGTON, VIRGINIA 22202-4704

April 30, 2005

MEMORANDUM FOR DIRECTOR, DEFENSE FINANCE AND ACCOUNTING SERVICE
DIRECTOR, DEFENSE INFORMATION SYSTEMS AGENCY

SUBJECT: Report on the Standard Finance System Controls Placed in Operation and Tests of
Operating Effectiveness for the Period October 1, 2004 through March 31, 2005
(Report No. D-2005-059)

We are providing this report for your information and use. No written response to this report is required. Therefore, we are publishing this report in final form.

We appreciate the courtesies extended to the staff. Questions should be directed to Ms. Addie M. Beima at (703) 428-1054 (DSN 664-1054) or Ms. Elaine M. Jennings at (703) 428-1055 (DSN 664-1055). If management requests, we will provide a formal briefing on the results.

By direction of the Deputy Inspector General for Auditing

Patricia B. Marsh
for Paul J. Granetto, CPA
Assistant Inspector General
Defense Financial Auditing
Service

Table of Contents

Foreword	i
Section I	
Independent Service Auditors' Report	1
Section II	
Information Provided by DFAS and DISA	9
Overview of Operations	9
Relevant Aspects of the Control Environment, Risk Assessments, and Monitoring	11
Control Environment	11
Risk Assessments	16
Monitoring	17
Information and Communication	19
Control Objectives and Related Control Activities	29
User Organization Control Considerations	30
Section III	
Control Objectives, Control Activities, and Tests of Operating Effectiveness	33
Scope Limitations	33
Control Deficiencies	33
Control Objectives, Control Activities, and Tests of Operating Effectiveness	34
General Computer Controls	
Security Program (SP)	34
Access Control (AC)	
Logical Security	46
Physical Security	60
Computer Operations	63
Change Control (CC)	67
System Software (SS)	78
Service Continuity (SC)	
Backup and Recovery	83

Physical Computer Asset Protection	85
Application Controls	
Authorization (AN)	87
Completeness (CP)	97
Accuracy (AY)	101
Integrity (IN)	109
 Section IV	
Supplemental Information Provided by DFAS and DISA	125
Continuity of Operations Planning	125
 Acronyms and Abbreviations	127
 Report Distribution	129

FOREWORD

This report is intended for the use of DFAS and DISA management, its user organizations, and the independent auditors of its user organizations. Department of Defense personnel who manage and use the Standard Finance System (STANFINS) will also find this report of interest as it contains information about STANFINS general and application controls.

The IG DoD is implementing a long-range strategy to conduct audits of DoD financial statements. The Chief Financial Officer's Act of 1990 (P.L. 101-576), as amended, mandates that agencies prepare and conduct audits of financial statements. The reliability of information in STANFINS directly impacts DoD's ability to produce reliable, and ultimately auditable, financial statements; which is key to achieving the goals of the Chief Financial Officer's Act.

STANFINS is a general fund accounting system developed to support day-to-day operations of U.S. Army and National Guard installations world-wide, as well as the Defense Commissary Agency. Other DoD agencies receive trial balance data from STANFINS for use in preparing their financial statements. STANFINS provides support for fund and obligation control, budget execution and expenditure accounting, reimbursable accounting, miscellaneous accounting (disbursements and collections), general ledger control, and financial reporting. In FY 2003, STANFINS processed more than \$300 billion of general fund transactions.

This audit assessed controls over the STANFINS processing of the \$300 billion of transactions at DFAS and DISA. This report provides an opinion on the fairness of presentation, the adequacy of design, and the operating effectiveness of key controls that are relevant to audits of user organization financial statements. As a result, this audit precludes the need for multiple audits of STANFINS controls previously performed by user organizations to plan or conduct financial statement and performance audits. This audit will also provide, in a separate audit report, recommendations to management for correction of identified control deficiencies. Effective internal control is critical to achieving reliable information for all management reporting and decision making purposes.

A selection process is underway to replace STANFINS with the General Fund Enterprise Business System (GFEBS). However, based on the status of the GFEBS procurement effort, it is not likely that GFEBS will replace STANFINS until after FY 2007. This audit will assist in ensuring that STANFINS provides reliable information to management in the interim and, when GFEBS does come on line, ensuring that only valid data is migrated to the new system.

Section I: Independent Service Auditors' Report



INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
400 ARMY NAVY DRIVE
ARLINGTON, VIRGINIA 22202-4704

APR 30 2005

MEMORANDUM FOR THE DIRECTOR, DEFENSE FINANCE AND ACCOUNTING
SERVICE
DIRECTOR, DEFENSE INFORMATION SYSTEMS AGENCY

SUBJECT: Report on Standard Finance System Controls Placed in Operation and Tests of Operating Effectiveness for the Period October 1, 2004 through March 31, 2005

We have examined the accompanying description of Defense Finance and Accounting Service (DFAS) and Defense Information Systems Agency (DISA) controls applicable to the Standard Finance System (STANFINS). Our examination included procedures to develop reasonable assurance that the DFAS and DISA controls that may be relevant to user organizations' internal control, as it relates to an audit of financial statements, are fairly presented in all material respects. We also determined whether the controls were suitably designed to achieve the control objectives, controls were followed, and user organization controls were contemplated in the design of DFAS and DISA controls. Additionally, we examined whether these controls were in operation as of March 31, 2005.

DFAS uses a series of end-user applications and software utilities and programs external to STANFINS including, but not limited to, the Databased Accounting Reconciliation System (DARS), Program and Budget Accounting System, and Structured Query Language (SQL)-like queries locally developed at various DFAS field sites to facilitate high-volume data input and enhance data querying capabilities. The mainframe computer that houses STANFINS is connected to and accessed by both DISA- and DFAS-maintained networks that are subject to separate and specific sets of control. The accompanying description includes only those controls and related control objectives of DISA and DFAS as applicable to automated STANFINS functionality (to include internal program functionality, automated reporting capabilities, and associated manual review and correction procedures performed by DFAS personnel) and the DFAS Enterprise Local Area Network (ELAN). It does not include control objectives and related controls applicable to locally configured end-user applications, software utilities and programs external to STANFINS, locally developed SQL queries, DISA network components, and centralized DFAS network components. Our examination did not extend to these controls.

The control objectives were specified by the Office of the Inspector General, Department of Defense. Our examination was performed in accordance with standards established by the American Institute of Certified Public Accountants and the standards applicable to financial audits contained in Government Auditing Standards issued by the Comptroller General of the United States, and included those procedures we considered necessary in the circumstances to obtain a reasonable basis for rendering our opinion.

As discussed in Section 3, *Control Objectives, Control Activities, and Tests of Operating Effectiveness*, the control description within this report, DFAS did not create or maintain documentation to support key controls over STANFINS processing of financial transactions. As a result, we found limited documentation of the following:

- Verification that key source documents such as Funding Authorization Documents (FADs), vouchers, and transmittal letters (with embedded transactions) submitted by installation management were authorized;
- Authorization for, and performance of, review and corrections to data errors and accounting issues; and

- Reviews to confirm that STANFINS transaction processing or master file updates were successfully completed, and that source documents were correctly entered into the STANFINS Terminal Application Processing System (TAPS).

Additionally, the STANFINS General Fund and Inquiry (AVK087) report, relied on by users to identify accounting issues such as Negative Unliquidated Obligations (NULOs) and problem disbursements, reported accounting issues only when automated edit checks first identified and reported the error. Issues were not reported on subsequent reports regardless of whether corrective actions were taken. This condition increased the risk that issues not addressed on the day of first reporting would not be addressed and would ultimately result in misstatements of financial information.

In our opinion, the accompanying description of the aforementioned controls presents fairly, in all material respects, the relevant aspects of DFAS and DISA controls that had been placed in operation as of March 31, 2005. Also, in our opinion, except for the deficiencies referred to in the preceding paragraph, the controls, as described, are suitably designed to provide reasonable assurance that the specified control objectives would be achieved if the described controls were complied with satisfactorily.

Key logical security controls were ineffectively operating and, in some cases, not implemented during a part or all of the examination period. Specifically:

- During testing, DFAS field sites were unable to generate STANFINS and TAPS user access lists directly from the security system, which prevented effective STANFINS logical access administration. Also, controls related to the authorization of logical access to the STANFINS application and General Support System (GSS) were inconsistently applied. Specifically, user access forms, including management authorization for user access, were inconsistently documented. User access recertifications were inconsistently performed across DISA and DFAS locations and, as a result, duplicate accounts, inactive accounts, accounts belonging to separated employees, and accounts with excessive access were identified across all STANFINS Army Standard Information Management System (ASIMS) domains.
- Technical control configurations restricting access to the STANFINS application and GSS did not comply with DoD requirements. Specifically, minimum password length, complexity requirements, and reuse restrictions and automated checking to verify the authority of users to submit batch jobs contained configured settings that did not comply with DISA policy. Remote access to the DISA Defense Enterprise Computing Center (DECC) mainframe located in St. Louis, Missouri, via telnet was not restricted or secured with encryption.
- Audit logging, monitoring, and follow-up were conducted inconsistently and were undocumented for three months of the six-month examination period. Specifically, audit logs were not created for the use of sensitive system utilities on the STANFINS domains secured by Computer Associates (CA) Access Control Facility 2 (ACF2) security software. Logs that detail activities of remote user sessions were not maintained or reviewed. Also, DISA had not segregated monitoring and security administration responsibilities for ACF2 and CA-Top Secret security software.

These control deficiencies had the potential to affect the achievement of application control objectives related to authorization and integrity, as well as the logical security control objective.

Additionally, authorizing officials inconsistently signed access forms that granted entrance privileges to the computer room housing the STANFINS mainframe. Individuals were identified who had unnecessary access to the computer room housing the STANFINS mainframe.

Documentation of testing, authorization, and communication of STANFINS application changes was inconsistently generated and maintained. Additionally, there was no automated application change management/version control software in place to maintain a history of changes to STANFINS. These

control deficiencies had the potential to affect the achievement of integrity and application change control objectives.

DISA had not developed procedures to manage system software changes. The procedures should have specified the personnel responsible for changes, methods to describe system software problems, and means of testing changes. In addition, the procedures should have provided for impact analyses, change approvals, implementation and verification procedures, and documentation requirements. System software change documentation did not always include detailed information about the change, to include testing results or impact analyses. These control deficiencies had the potential to affect the achievement of the computer operations and integrity control objectives, as well as the system software control objective.

As discussed in the accompanying control descriptions, key computer operations controls were ineffectively operating and, in some cases, not implemented during a part or all of the examination period. Specifically:

- At DECC St Louis, Missouri, user access to Control-M (a mainframe job scheduling utility) was excessive based on segregation of duties principles.
- One DFAS site responsible for production administration had not documented production scheduling procedures. The site lacked procedures for scheduling and monitoring production jobs and handling job failures.
- Two of three DFAS sites responsible for production administration did not have documented procedures for job schedule changes.


In addition to the procedures we considered necessary to render our opinion as expressed in the previous paragraph, we applied tests to specific controls, listed in section III, to obtain evidence about their effectiveness in meeting control objectives, described in section III, during the period from October 1, 2004 to March 31, 2005. The specific controls and the nature, timing, extent, and results of the tests are listed in section III. This information has been provided to user organizations of DFAS and DISA and to their auditors to be taken into consideration, along with information about the internal control of user organizations, when making assessments of control risk for user organizations. In our opinion, except for the deficiencies listed in the preceding paragraphs, the controls that were tested, as described in section III, were operating with sufficient effectiveness to provide reasonable, but not absolute, assurance that the control objectives specified in section III were achieved during the period from October 1, 2004 to March 31, 2005; however, the scope of our engagement did not include tests to determine whether control objectives not listed in section III were achieved; accordingly, we express no opinion on the achievement of control objectives not listed in section III.

The relative effectiveness and significance of specific controls at DFAS and DISA and their effect on assessments of control risk at user organizations are dependent on their interaction with the controls and other factors present at individual user organizations. We performed no procedures to evaluate the effectiveness of controls at individual user organizations.

The description of controls at DFAS and DISA is as of March 31, 2005, and the information about tests of the operating effectiveness of specific controls covers the period from October 1, 2004 to March 31, 2005. Any projection of such information to the future is subject to the risk that, because of change, the description may no longer portray the controls in existence. The potential effectiveness of specific controls at DFAS and DISA is subject to inherent limitations and, accordingly, errors or fraud may occur and not be detected. Furthermore, the projection of any conclusions, based on our findings, to future periods is subject to the risk that changes made to the system or controls, or the failure to make needed changes to the system or controls, may alter the validity of such conclusions.

DFAS and DISA present the information in section IV of this report to provide additional information and is not a part of DFAS and DISA descriptions of controls placed in operation. The information in section IV has not been subjected to the procedures applied in the examination of the description of the controls applicable to the processing of transactions for user organizations and, accordingly, we express no opinion on it.

By direction of the Deputy Inspector General for Auditing:


for Paul J. Granetto, CPA
Assistant Inspector General
Defense Financial Auditing
Service

Section II: Information Provided by DFAS and DISA

II. Information Provided by DFAS and DISA

A. OVERVIEW OF OPERATIONS

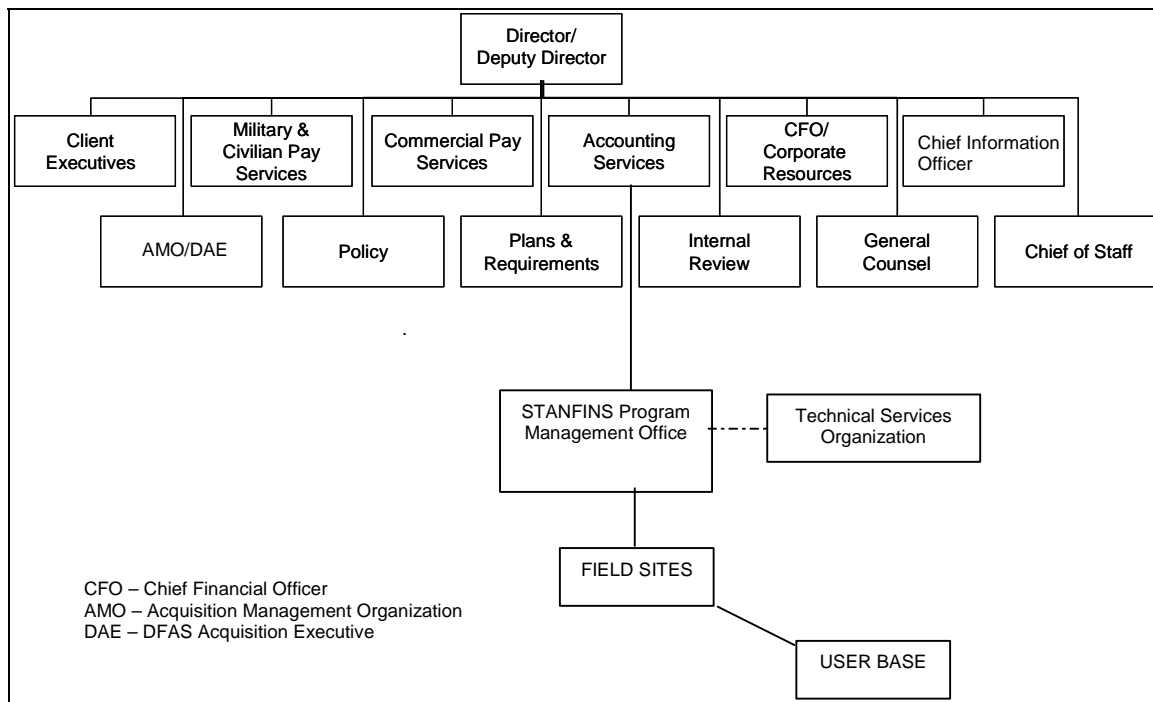
Department of Defense

The Department of Defense (DoD) is the cabinet-level agency responsible for establishing and administering defense initiatives and strategy for the United States. DoD employs approximately two million military and civilian individuals and has an annual revenue/operating budget of \$371 billion.

The DoD organization structure is arranged such that the Joint Chiefs of Staff, DoD OIG, Office of the Secretary of Defense, and each of the military branches report to the Secretary of Defense and Under Secretary of Defense.

Defense Finance and Accounting Service

The DFAS mission is to provide responsive, professional finance and accounting services for the DoD. The Director of DFAS reports to the Under Secretary of Defense Comptroller/Chief Financial Officer (USD(C)/CFO). DFAS is organized underneath the Office of the Secretary of Defense and is responsible for the proper accounting of resources within DoD. DFAS is organized such that the Director and Deputy Director of DFAS oversee operations carried out as depicted below:



Within the Accounting Systems Directorate, Installation and Tactical Support Accounting Systems Organization, the Program Management Office (PMO) helps to ensure continued operation of STANFINS in accordance with DoD security and operational requirements. The Technical Services Organization (TSO) is responsible for elements of the technical administration of STANFINS and provides multi-tier system support in coordination with other organizations. The TSO carries out its

responsibilities for many aspects of system support in coordination with the Centralized Directorate for Information Management (CDOIM), as well as decentralized DOIM organizations servicing other DFAS sites. CDOIM and DOIM groups are responsible for the overall management and continuance of the STANFINS computer processing operations. See the Information Systems section (in the Information and Communication section) for a detailed description of PMO, TSO, CDOIM, and DOIM organizational roles relative to the administration and operation of STANFINS.

Defense Information Systems Agency

DISA is a combat support agency responsible for planning, engineering, acquiring, fielding, and supporting global net-centric (systems with operations distributed across a network) solutions to serve the needs of the President, Vice President, the Secretary of Defense, and other DoD Components, under all conditions of peace and war.

DISA performs the following in support of the administration of STANFINS underlying information technology architecture:

- Installation and maintenance of system software, including operating systems, communication networks, and file control software;
- Installation and maintenance of the ASIMS database management software, as well as CA's Data Query (a Commercial Off-the-Shelf (COTS) software package);
- Administration of system parameter settings available within the ASIMS software, which provides logical access control;
- Restriction of physical access to computer facilities and application programs/data files housed in the facility;
- Backup and contingency planning, including maintenance of off-site processing capabilities and rotational off-site storage of critical files; and
- Logical segregation of major applications from other systems resident on the domain hardware and from unauthorized external users.

By providing services and fulfilling responsibilities outlined above, DFAS and DISA represent service organizations/service organization components that act in concert to provide finance and accounting services supported by information systems and technology to specific DoD user organizations:

- Army Posts, Camps and Stations (e.g., Fort Riley, Fort Belvoir)
- Air Force (Security Assistance – DFAS-Denver)
- Defense Commissary Agency (DeCA) – Worldwide
- Other Defense Agencies (e.g., Defense Advanced Research Projects Agency (DARPA) and DoDEA)
- DFAS field sites (e.g., Pearl Harbor, HI; San Antonio, TX; Indianapolis, IN; Orlando, FL; Rome, NY; Lawton, OK; Seaside, CA)

DISA's relationship with DFAS is, itself, a service organization/user organization relationship. DISA provides platform hosting and systems and hardware support services to DFAS, a user/administrator of the STANFINS application resident on the DISA-operated platform; however, for the purposes of the Statement on Auditing Standards (SAS) 70 examination (the results of which are reported herein), DISA and DFAS are viewed as a combined service organization delivering information systems technology-enabled finance and accounting support services, which are in part realized through the STANFINS application and GSS, to a series of user organizations.

B. RELEVANT ASPECTS OF THE CONTROL ENVIRONMENT, RISK ASSESSMENTS, AND MONITORING

Control Environment

Defense Finance and Accounting Service

The structure of the organizations supporting STANFINS provides the overall framework for planning, directing, and controlling operations. Operations and business functions are segregated into tasks and/or staffs according to job responsibilities. This framework allows STANFINS users to clearly define the lines of authority for reporting and communication purposes, and allows employees to focus on the business functions of their respective divisions.

Administrative and user groups are organized by function to maintain an appropriate segregation of duties, which promotes checks and balances for key steps in all sensitive functions and meets applicable legal and regulatory requirements. Segregation of duties covers, wherever possible, both employees and supervisors. In general, different individuals perform key steps in completing all major types of financial transactions. These steps include budgeting, preparation of proposals or requisitions, authorization of transactions, certification of funds availability, obligation of funds, recordation of obligations, certification of disbursements (or schedules of disbursements issued by the Treasury Department), disbursement of funds, and financial reporting.

TSO-Indianapolis manages the STANFINS Information Technology (IT) security program, which is focused on assuring that STANFINS' infrastructure and critical assets are appropriately safeguarded. The Program/System Manager provides overall leadership and helps coordinate policies, procedures, and activities with IT services. The program is administered based on a fundamental philosophy of risk management, whereby IT risks are identified, understood, assessed, and mitigated appropriately. This planned approach allows the Information Systems Security Manager (ISSM) to implement appropriate protective measures and helps ensure the privacy, availability, integrity, and security of IT resources (See the Risk Assessments section for more information regarding this process).

STANFINS senior IT staff, acting under the direction of the ISSM develop and implement Army-wide IT security, oversee certification and accreditation of the STANFINS mission essential systems, establish and implement the STANFINS-wide Incidence Response Program, to include investigating reported IT security incidents, and their appropriate disposition.

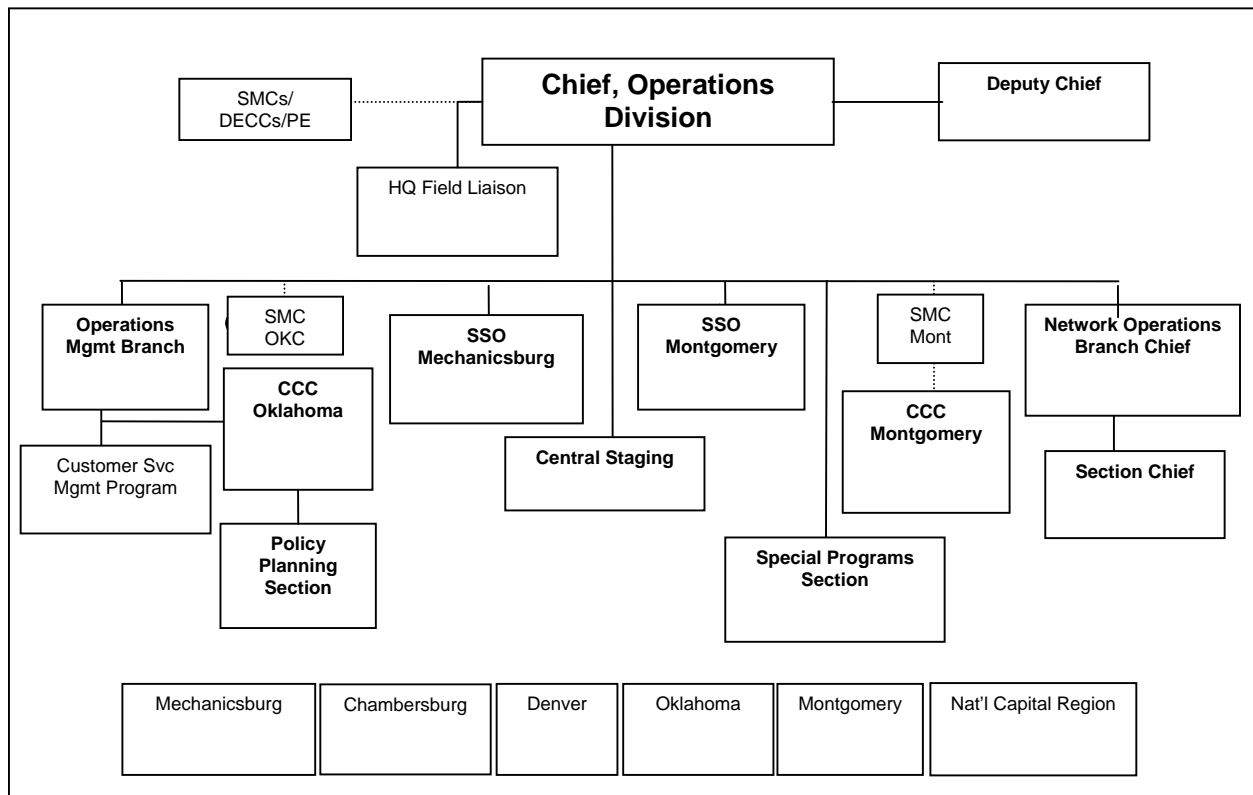
Defense Information Systems Agency

Operations

Operations has the responsibility of providing Computing Services core services and meeting customer expectations through professional, consistent operations services and standard implementation of proven industry best practices. The Computing Services Operations Division (CSOD) is responsible for continual refinement and analysis of operations performance metrics and practices to identify and implement opportunities for improvement in the execution of core operations services and maintaining the integrity of the security posture of the operations environment. The implementation of a strong customer-focused environment and highly responsive post-deployment support services maintains and supports Computing Services customer relationships. Centralized management of all operating locations helps to ensure that customers receive the same predictable high quality services regardless of processing location.

Computing Services Operations Division Headquarters

DISA Computing Services Operations is organized in three layers: Policy/Plans at the Headquarters, centralized operations at Headquarter, and the direct operations functions at field operating locations. The overall organization is depicted in the following chart.



SMC = Systems Management Center
DECC= Defense Enterprise Computing Center
CCC = Central Communications Center
SSO = Systems Support Office
PE = Processing Elements

At the CSOD Headquarters-level, the Chief Operations Officer reports directly to the Principal Director for DISA Computing Services. The Chief of Operations has overall responsibility for issuing operations standards, policies, plans, standard business processes, and standard operations procedures.

Accomplishing the objectives of the core CSOD function requires extensive interaction with all other organizational headquarters elements, senior level customer representatives, and other DISA elements.

Network Operations Branch

Current Operations is an Headquarters-level function providing a centralized enterprise monitoring function to provide an enhanced situational awareness posture of the entire Computing Services operations environment for senior level management. This function supports the corporate incident reporting process that provides details of high impact, high visibility, or high interest incidents throughout the operational environment, as well as providing a liaison function with other key elements of DISA to

help ensure that DISA elements and DISA CSD maintain mutual awareness of incidents that cross organizational boundaries.

Special Programs Section – Application Support and Security

The Applications Support team serves as Operations representatives on new business proposal teams. They consult with customers to identify and specify system requirements, define systems scope and objectives, and prepare estimates of the operational resources that will be required for sustainment. Responsibilities include monitoring, analyzing, and reporting performance metrics, outages, and trends for the production systems associated with assigned functional support areas.

The Security Team provides Information Assurance guidance and enforces policy. They also provide centralized clearance processing for CSOD personnel security as matrixed support from the Field Security Office (FSO).

Operations Management Branch

The Operations Management Branch is attached to the Chief of Operations at the Headquarters level. This organization is responsible for policies, procedures, standards, and management oversight for the CSOD configuration management process. The Policy/Planning Branch is responsible for the centralized change management process within Computing Services and manages the enterprise Configuration Control Board.

The Operations Management Branch includes centralized technical and program support functions impacting standardization and optimization of the operating site production environments. Denver, Colorado and Mechanicsburg, Pennsylvania currently support CMS, Capacity Management, and Multiple Virtual Storage (MVS) Capacity functions. Specific functions include: capacity management for all platforms, performance management, asset management, inventory management, facilities management, assured computing, quality management, and customer service management.

Central Staging

The Central Staging Site is also a part of this branch and will perform centralized receipt and staging of enterprise assets. The Central Staging Site is responsible for inventory control and asset management for all new Computing Services assets.

Centralized Operations

Operations functions providing support services that impact all platforms and customers are organized as centralized operations functions at the Headquarters level. The centralized functional organizations are the System Support Offices and the Production Branch of CSOD.

System Support Office (SSO)

Mechanicsburg and Montgomery support the SSO functions. SSO Mechanicsburg provides executive software standards for OS/390 platforms, chairs the Executive Software Change Control Board, and maintains a software library of all OS/390 products and patches. SSO Mechanicsburg also provides consultation and technical support for special projects impacting the OS/390 environment and a help desk function that acts as a liaison for operating locations needing technical assistance from vendors whose products the DISA CSD Central Maintenance contract supports. SSO Montgomery provides similar executive software support functions for the Unisys and Open Systems environments and maintains a

library of software for these platforms. The SSO supported Software Factory provides an online mechanism for the software release process. SSO Montgomery also provides a release process for distribution of physical media.

Central Communications Centers (CCCs)

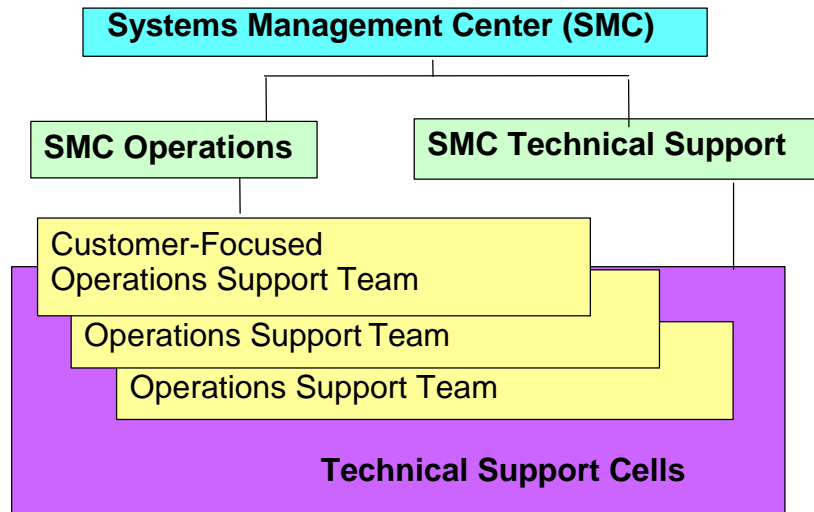
The CCCs are located at two of the Systems Management Centers (SMCs). The CCCs provide geographically diverse coverage to support the technical network infrastructure operations functions.

Systems Management Centers/Defense Enterprise Computing Centers (SMC/DECCs)

Production Operations incorporates the field operations functions directly supporting customer requirements. Four SMC locations and four production sites support Production Operations. The SMC locations include production operations as well as the technical support and standardized customer support functions for the enterprise. The four production sites provide facilities and touch labor, but one of the SMC locations remotely provides technical support and customer support functions for systems residing at these production sites.

SMC operating facilities are located at four production operations sites. Two SMCs support OS/390 processing, two support UNISYS processing, and all four sites support server workload. Each SMC provides both production processing and technical support for the applicable operating system platforms. Two SMCs also have a Central Communications Center providing technical network management for all production sites. Each SMC provides customer support services focused on specific customer groups. The primary customer support groups are the Navy, Marine Corps, Air Force, Army, DFAS, Defense Logistics Agency (DLA), and Military Health Services (MHS).

Core operations and customer support functions are organized in two branches within each SMC: SMC Operations and SMC Technical Support. The relationship of these organizational elements is illustrated below.



SMC Operations

Consistent with industry practice, the DISA CSD Operations Support Team (OST) concept provides a customer-oriented service structure to implement high performance help desks. Under this concept, a customer-focused team is constructed to provide all the service and knowledge elements that pertain to that customer's post-deployment support. These services include the traditional Tier 1 help desk support, traditional basic console/operations support for the customer's applications, basic system monitoring for the customer's platforms and applications, and other key skills required to be responsive to that customer.

The availability of a higher set of knowledge and skills co-located in the OST improves First Call Resolution (FCR). Incorporation of the basic applications support, scheduling, and operations functions for the customer also promote an intimate knowledge of that customer's environment, priorities, and an immediate knowledge of current status. Incorporation of monitoring functions using Enterprise Systems Management (ESM) standard system monitoring components oriented toward the OST customer completes a situational awareness for that customer that ensures a high quality professional response at the first call. Only issues that require system level access or that are new unique problems will have to be referred to the technical support group.

Customer-oriented OSTs provide a single phone number and a consistent team of individuals to assist the customer base. This results in the development of a relationship of trust and loyalty with the customer and an in-depth understanding of customer missions, concerns, and operations cycles. Often, agent monitoring systems will be able to take action proactively because of this level of customer knowledge. The development of a close relationship with the customer, and the dedication of a team to that customer, promotes an implementation of Total Contact Management that supports SMC operations objectives.

With the OST focus on a particular customer, trends in types of calls will become apparent. Knowledgeable agents experienced with a particular customer base will be able to identify candidate

categories for further analysis, either perform the analysis or refer to the proper technician, and help define permanent fixes to eliminate categories of calls. Through their relationship with the customer, the OST can perform customer education over time to help eliminate other categories of routine calls. They can also support online self-help by providing knowledge suitable for the customer to access directly to answer common questions. These activities will eventually result in call prevention for routine issues or informational inquiries. As agents filter out routine calls, they will be devoted to resolving increasingly complex questions for their customers.

Risk Assessments

Defense Finance and Accounting Service

Management representatives of the PMO and TSO, collectively known as “STANFINS management,” identify and evaluate relevant risks associated with operations and systems. STANFINS management is aware of the numerous internal and external risks associated with STANFINS operations and takes appropriate action to eliminate or mitigate the risk exposure. STANFINS management meets continuously to discuss division operations. Management addresses risk identification, analysis, and resolution planning and implementation. Risks identified through external audits and other evaluations, including the Department of Defense Information Technology Security Certification and Accreditation Process (DITSCAP) (described in the Monitoring section), are also included in the risk assessment process.

STANFINS Management follows the Mission Assurance Category (MAC) III controls assessment guidelines and Confidentiality Controls as documented in DoD Instruction 8500.2, *Information Assurance Implementation*, when performing risk assessment activities. STANFINS Management performed the most recent risk assessment in November 2003, which is documented in Appendices P and Q of the STANFINS System Security Authorization Agreement (SSAA). The Information Assurance division of STANFINS Management performed this MAC III-based assessment. The MAC III assessment evaluates existing policies and procedures, and provides a summary of areas of potential risk that relate to STANFINS.

Defense Information Systems Agency

Risk Assessments have been developed for each enclave/site within Computing Services that identifies the risk, probability of the risk occurring, and impact if the risk does occur; identifies countermeasures implemented to reduce the risk; and identifies the residual risk, potential risk, and countermeasures required to address the potential risk. These risk assessment documents are updated a minimum of every 18 months.

Sites are capable of performing self-assessment Security Readiness Reviews (SRR) that validate compliance with Security Technical Implementation Guides (STIGs) and can perform self-assessment vulnerability scans.

Field Security Operations conducts annual independent reviews for STIG compliance and vulnerability scans.

Monitoring

Defense Finance and Accounting Service

DFAS, TSO, and DISA management and supervisors perform continuous monitoring of the performance of internal controls as a part of their normal operations. They use reconciliation, comparisons, and exception reporting, along with normal supervisory activities to achieve internal control monitoring. Management evaluates findings from external audits and management reviews, develops corrective actions or responses, and takes action to resolve the findings. They report the status of the resolution of the material findings and weakness to DFAS-IN STANFINS Systems Office on a regular basis and action is taken as necessary. In addition, the DITSCAP Certification and Accreditation (C&A) requirements include the periodic monitoring of STANFINS-related internal controls.

DoD Instruction 5200.40, *Department of Defense Information Technology Security Certification and Accreditation Process*, December 20, 1997, establishes a standard Department-wide process, set of activities, general tasks, and management structure to certify and accredit information systems that will maintain the information assurance and security posture of the defense information infrastructure throughout the lifecycle of each system. The certification process is a comprehensive evaluation of the technical and non-technical security features of an information system and other safeguards to establish the extent to which a particular design and implementation meets specified security requirements and covers physical, personnel administrative, information, information systems, and communications security. The accreditation process is a formal declaration by the designated approving authority that an information system is approved to operate in a particular security mode using a prescribed set of safeguards at an acceptable level of risk. STANFINS has been certified and accredited by the DFAS Designated Authority in December, 2003.

Defense Information Systems Agency

The CSOD Current Operations staff provides centralized event monitoring in support of the CSD senior management. Standard monitoring tools provide near real-time data on the status of all production operations environment components including applications, platforms, and networks. Enterprise Systems Management (ESM) provides presentation tools that allow monitoring of consolidated information by customer, application, network segment, or by any other appropriate business category designation. The Operations Monitoring function maintains a continuous surveillance of high-level indicators of the health of the key elements of the CSOD operations environments. Alerts and alarms provide an early warning of potential customer impact and enhanced situational posture awareness for the Chief of Operations and senior CSD staff.

Information Assurance (IA) Security staff is specifically charged with providing information security support and solutions for intrusion monitoring and detection, incident reporting, and trend analysis in support of customer requirements. The IA staff participates in the planning, installation, operations, and maintenance of Information Security technologies, systems, procedures, plans, and services associated with each customer's Area of Responsibility. The day-to-day operations for security provided by IA include, but are not limited to, the following core functions:

- Network Intrusion Detection Monitoring
- Level I data analysis – Correlation of activity with sensor data and initial log review
- AOR Incident/Event Trending
- Event, Incident, and Mission impact determination/escalation/prioritization
- Coordination of Incident & Event Feedback to customer
- Penetration Tests/IA Exercises/IA Reviews,

In accordance with DISA Instruction 630-230-31, *Enclave Security*, March 30, 2001, IA technology has been implemented throughout the DISA Assured Computing Environment in order to provide a reliable, available, and secure network. Other IA tools, processes, and functions may be implemented as deemed necessary to defend the network, enclave boundaries, local computing environments, and supporting infrastructure against all threats.

C. INFORMATION AND COMMUNICATION

Information Systems

Application Overview

STANFINS is a general fund accounting system developed to support the day-to-day operations of the U.S. Army, as well as other select DoD operational components. STANFINS provides for the input and master file update of transactions related to funding and budget execution, expenditures, “reimbursables,” disbursements and collections with no impact on funds allotted to installations, and general ledger updates for the purposes of complete and accurate financial reporting. STANFINS shares the hardware and telecommunications resources of ASIMS, and 65 DECC-St. Louis databases currently field the system.

The Director, Finance and Accounting, Office of the Assistant Secretary of the Army for Financial Management (OASA (FM)) and the U.S. Army Information Systems Software Development Center–Washington developed STANFINS through a joint effort. STANFINS design has been predicated on the OASA (FM) requirement to help ensure that the Department of the Army accounting systems comply with the Budget and Accounting Procedures Act of 1950.

Specifically, STANFINS provides the following:

- Full disclosure of the financial results of all activities
- Adequate information required for all management purposes
- Effective control over and accountability for all funds and other assets
- Reliable data to serve all budgetary purposes
- Means for integrating Army financial data with related data in the accounts of the Treasury Department.

STANFINS is a legacy system operating in a “maintenance mode” (i.e., only emergency changes are applied to the application production environment). Although in maintenance mode, STANFINS systems offices and field sites are consolidating databases to realize savings and migrate new customers to STANFINS such as the National Guard and the Installation Management Agency (IMA). A selection process is currently underway to replace STANFINS and many other systems supporting Army customers with a new Enterprise Resource Planning software package: the General Fund Enterprise Business System.

General Support System

STANFINS production programs (also known as “jobs”) exist on a Complimentary Metal Oxide Semiconductor (CMOS) AMDAHL 2054 mainframe running IBM’s OS/390 Release 2.10 mainframe operating system. Each Logical Partition (LPAR) contains a series of site/installation databases that are configured to a one database to one site/installation ratio. The mainframe is responsible for storing all STANFINS data with interactive capability for local and remote end-users. The mainframe uses removable media for data storage. IBM compatible personal computers with terminal emulation software clients are used to input data not entered through automated interfaces with other systems. All end-user connectivity transmit clear text non-encrypted data using the ELAN and the Sensitive but non-classified Internet Protocol Router Network (NIPRNET), a telephone/telecommunication media-based network managed by DISA. The mainframe connects to the network communication devices that comprise the gateways to the NIPRNET and ELAN via IBM Open Systems Adapter integrated adapter hardware and software.

STANFINS programs are written in Common Business Oriented Language 74 and comprise approximately 1.8 million lines of code that are designed to run on IBM/MVS/XA processing environments. The TAPS and Customer Information Control System (CICS) provide for and facilitate online user interaction with the application. CICS is an online, interactive, mainframe program used to access various applications. CICS permits entry and update of information on a screen, the movement between screens, and the printing of documents. The TAPS utility is used during sign-on and sign-off procedures to the ASIMS Network and for the manual input of accounting data into STANFINS. COTS software provides Data Query capability. BMC Software's Control-M utility provides production scheduling and management. CA DATACOM/database is the backend database management system that contains STANFINS standing and transaction data.

Each STANFINS-related LPAR resident on the CMOS7 mainframe contains a series of site/installation databases that are currently configured at a one database to one site/installation relationship. There are 65 databases established on six production LPARs. Three of these databases, which are classified, are outside of the scope of this review. The six production LPARs, along with one development LPAR, are identified as follows:

Domain Code	Domain Name	Applicable DFAS Field sites	Installation Databases
MSK-ASIMS-S	St. Louis	<ul style="list-style-type: none"> • San Antonio, TX • Lawton, OK • Directorate for Network Operations (DNO), Indianapolis, IN • Rome, NY • Orlando, FL 	<ul style="list-style-type: none"> • Fitzsimons • Ft. Carson • Ft. Hood • Ft. Sam-Houston • National Guard Bureau (NGB) Oklahoma • Ft. Leavenworth • Ft. Polk • Ft. Riley • Ft. Sill • Ft. Buchanan
MSL-ASIMS-E	East	<ul style="list-style-type: none"> • Columbus, OH • DNO, Indianapolis, IN • Centralized Disbursing • Rome, NY • Orlando, FL • Military Pay (MILPAY) • Lexington, KY • Lawton, OK • DEPT97 	<ul style="list-style-type: none"> • Europe DeCA • Columbus DeCA • Disbursing • Secretary of the Army Financial Operations (SAFINOPS) • Ft. Campbell • Carlisle Barracks • Ft. Dix • Ft. Drum • DFAS-IN Harrison • Centralized Pay (CEN PAY) • NGB Pennsylvania • United States Army Intelligence and Security Command (INSCOM) • Ft. Knox • U.S. Army Special

Domain Code	Domain Name	Applicable DFAS Field sites	Installation Databases
			<ul style="list-style-type: none"> Operations Command (USASOC) • Ft. Meade • Defense Travel System (DTS) • Ft. Leonard Wood • DFAS
MSM-ASIMS-W	West	<ul style="list-style-type: none"> • Pearl Harbor, HI • Seaside, CA • DNO, Indianapolis, IN • Rome, NY 	<ul style="list-style-type: none"> • Alaska/Hawaii • Ft. Huachuca • Ft. Bliss • NGB-Indiana • Ft. Irwin • NGB-California • Ft. Lewis • Reserves
MSQ-ASIMS-Ch	Chambersburg	<ul style="list-style-type: none"> • DNO, Indianapolis, IN • San Antonio, TX • Rome, NY • Seaside, CA • Lawton, OK • Norfolk, VA • DFAS-Denver 	<ul style="list-style-type: none"> • Military District of Washington (MDW) • Foreign Military Sales (FMS) • Ft. Eustis • Europe-Medical Command (MEDCOM) • Europe-Kaiserslautern, Germany (KTOWN) • Defense Lang Institute • West Point • Walter Reed • Ft. Detrick • Ft. Belvoir • Inst. Mgmt Agency-Outside of the Continental United States (OCONUS) • Ft. Devins • Ft. Lee
MSW-JAK	JAK (Japan-Korea)	<ul style="list-style-type: none"> • Yakota, Japan • Seoul, Korea 	<ul style="list-style-type: none"> • Japan • Korea
MQC-ASIMS-T9	Supports STANFINS Development	N/A	N/A
MQD-ASIMS-H	Huntsville	<ul style="list-style-type: none"> • Rome, NY • Lawton, OK • DNO, Indianapolis, IN • Orlando, FL • Lexington, KY 	<ul style="list-style-type: none"> • Ft. Bragg • Installation Management Agency (IMA) East • IMA West • Ft. Gordon • NGB Alabama • Ft. Jackson

Domain Code	Domain Name	Applicable DFAS Field sites	Installation Databases
			<ul style="list-style-type: none"> • Ft. McPherson • Ft. Rucker • Ft. Stewart • Kuwait • United States Military Training Mission (USMTM)-Saudi

Information Security

STANFINS is an unclassified Army-wide standard accounting system. The technical implementation of information security has been applied to STANFINS at various levels of the GSS (i.e., workstations, servers, hosts, operating systems, network/communication devices, etc.) and application architecture. In accordance with DoD Directive 8500.1 and DoD Instruction 8500.2, the MAC for this system has been determined to be MAC III. The confidentiality level of the system is Sensitive. All data processed by STANFINS is sensitive but unclassified data. The loss, misuse, or unauthorized access to or modification of this information could adversely affect the national interest or the privacy to which individuals are entitled under section 552a of Title 5, United States Code (The Privacy Act).

Users access STANFINS at IBM-compatible workstations that contain terminal emulation software enabling them to connect to the STANFINS-resident mainframe via their local area network (LAN) server gateway and the NIPRNET government communications network. Physical access controls to DFAS sites and desktop operating system security are applied to restrict access to authorized individuals at the local workstation level. The application of least-privilege and need-to-know information security principles, utilization of user ID and password security, configuration of operating system/server security settings in accordance with DoD security implementation guidelines, and implementation of physical access controls to communications devices and lines provide network-level security that restricts access to ELAN and NIPRNET resources (including STANFINS access points) to authorized individuals.

Users connect to the mainframe and their STANFINS application/databases instance by accessing and being validated by Computer Associate's Access Control Facility 2 (ACF2) and CA-Top Secret Security¹ mainframe security software product. ACF2 and Top Secret are programs that enable security control and facilitate security administration in compatible mainframe environments. Physical access controls implemented at the DECC-St. Louis augment the application of the technical controls described in this paragraph.

Application Functionality

STANFINS is a general ledger containing all financial transactions for the customers it serves, largely Army installations. Financial data includes, but is not limited to, military and civilian pay transactions, cash accountability, vendor and commercial pay, travel pay, and funding. STANFINS records obligations, funds authorization, disbursements, accruals/expenditures, billings and collections, and reimbursables. Of special note, STANFINS was *not intended* to provide commitment accounting,

¹ CA-Top Secret Security mainframe security software package is used to restrict access to the Japan and Korea Logical Partitions (LPARs). The remaining LPARs are secured using ACF2.

budgetary accounting, or funds control. STANFINS records what has transacted but does not *automatically* control what has transacted.

Inputs to STANFINS

STANFINS accepts data in one of two ways.

1. Manual entry via TAPS. TAPS provides real-time online edits for data values. A warning appears if a data element or combination of data elements is incorrect. For example, if an Account Processing Code (APC) is not valid, a warning message will appear; however, users have the ability to bypass the warning and continue processing the transactions. Because STANFINS is a batch system, the APC code may not yet have been posted to the master file. So, it is a timing issue. If the user fails to enter the APC in the APC master, the transaction will fail and appear on a daily prelim report. A supervisor or “reconciler” obtains the Daily Preliminary Balance (AVK018) report and reconciles failed transactions. The “reconciler” is a different person than the input person.
2. Automated interface/file load². STANFINS receives files in one of three formats: qam (80 character from field site), nam (80 character from Installation), or DeCA (200 character). Currently, not all interface files into STANFINS are fully automated. Field site users have the ability to pull down a file, modify it, and then load it into STANFINS. Generally, a PC-based Microsoft Access database performs this offline function for the purpose of putting it into the correct format; however, as in any manual process, there is a risk that the data is modified rather than just reformatted.

Activities within STANFINS

Accounting transactions must be recorded and reported in the accounting period (month) in which they occur. The system automatically generates the General Ledger effect for each detail transaction based on the Type Action code of the transaction and other applicable direct or indirect input data including the APC, Element of Resource (EOR), Standard Document Number, and FY. The effect of these relationships is captured as a G/L Proforma Code, which defines the General Ledger account effects.

Outputs from STANFINS

STANFINS outputs can be categorized as follows:

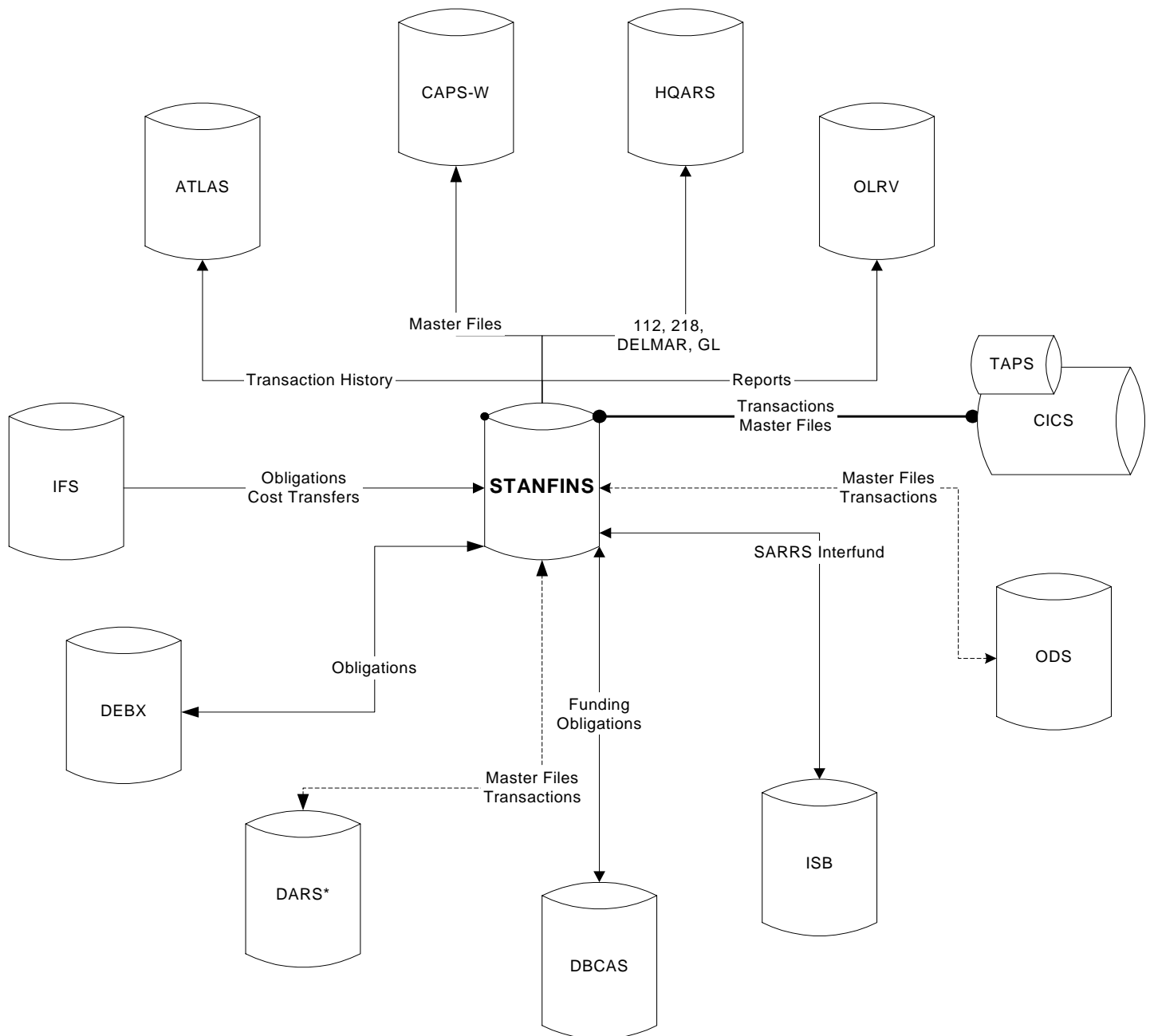
- (1) Reports/Queries. STANFINS produces a variety of reports and queries using the Online Report Viewer (OLRV), including exception reports, management reports, and financial reports. The system produces these reports on a daily, weekly, monthly, and/or as-required basis to provide information that is current and available when needed. Report files can also be sent to the CORP File Transfer Protocol (FTP) servers for use in DARS.
- (2) Interface Files. STANFINS sends interface files to three places:
 - Operational Data Store (ODS);
 - CORP1 or CORP2 – FTP servers in Information Services Organization (ISO) and TSO respectively. CORP1 is for other field sites. CORP2 is for the DNO; or
 - Installations’ servers.

Various systems and/or users use the outgoing interface files for various purposes. Examples include using the obligation information to determine if a disbursement can be made, matching the obligation to the funded amount, and providing updated master file tables.

² May have manual intervention.

Interfacing Systems

The following table documents systems that directly interface with STANFINS, as well as the nature of the interface and other relevant information:



*DARS and ATLAS are not “systems” per se but PC-based utilities that send and/or receive data from STANFINS for various purposes.

Interfacing System	Receive from STANFINS	Send to STANFINS	Nature of Interface	Notes
TAPS/CICS		✓	Location-to-location copy within the same mainframe	Front-end tool that facilitates/provides capabilities to manually input accounting data into STANFINS.
Accounting Transaction Ledger Archival System (ATLAS)	✓	✓	FTP	A queriable PC-based historical database tracking all transactions (funding, obligations, accruals, and disbursements) entering STANFINS via historical master files.
Computerized Accounts Payable System (CAPS)	✓		FTP	System uses the Account Processing Code Master file AXWAVK from STANFINS to provide accounting classification data used to make payments to vendors.
Databased Accounting Reconciliation System (DARS)	✓	✓	FTP	PC-based system receiving STANFINS historical master data files for research and possible mass correction of transactions previously entered into STANFINS. The files used by DARS are received and sent. Process is usually initiated in each of the Systems Offices of the field site from DECC-St. Louis.
Databased Commitment Accounting System (dbCAS)	✓	✓	FTP	PC-based Commitment Accounting System creating commitments, thus creating candidate obligation transactions used by STANFINS. During the STANFINS daily batch cycles, output files are created and sent to each of the dbCAS field site offices for distribution throughout their network. STANFINS passes the confirmation of the obligation entered into STANFINS (successful processing), and when the disbursement information is processed into STANFINS, the disbursement information is then passed to dbCAS to complete the cycle. Process is usually initiated in each of the Systems Offices of the field site from DECC-St. Louis.
Customer Automation and Report Environment (DEBX)	✓	✓	FTP	EDI transaction facilitation system; obligation acknowledgements are sent to STANFINS or DEBX, purchase card obligations received by DEBX are sent to STANFINS. DECC-Ogden, Utah runs DEBX, which receives X-12 standard UDF files and

Interfacing System	Receive from STANFINS	Send to STANFINS	Nature of Interface	Notes
				creates user specific system UDF for batch input into STANFINS. The files are in clear text STANFINS specific formats for processing obligations, accruals, and disbursement. These files are sent to DECC-St. Louis, Chambersburg, Rock Island (East or West), Huntsville, and the Far East.
Headquarters Army Reporting System	✓		FTP	System receives Status, Expenditure, and General Ledger report data form STANFINS during the month-end and year-end processing.
Integrated Facilities System-Modified		✓	FTP	System provides STANFINS cost distribution (obligation, accrual, and disbursement) data for the facility engineers at each post, camp, and station worldwide.
Installation Supply Buffer (ISB)		✓	FTP	ISB passes logistic financial transactions including obligations, accruals, disbursements, and interfund bills. U.S. Army Wide CONUS, OCONUS Installation (36 databases), DFAS-IN field sites (Rome, Orlando, DNO, Lexington, Lawton, Seaside, Europe), Norfolk, Pacific, Japan, San Antonio, and U.S. Army Reserve use ISB.
Operational Data Store	✓	✓	FTP	Sends STANFINS Obligations, Accruals, Payables, Accounts Receivable, Expenses, and Disbursements, and in turn receives transactional historical data. ODS is a major conduit for external interfacing systems, including SRD1, CAPS, DCD/DCW, DDRS, MOCAS, DJMS, DCPS, FAS, TAMMIS, AFMIS, ACIIPS, IATS, and others. Data is transmitted on a daily basis both as a sending system and a receiving system.
On-Line Report Viewing	✓		FTP	Commercial Off-the-Shelf, Report Dot Web provides users reports modeled after STANFINS reports.

STANFINS Support Organizations

The PMO, headquartered at DFAS-Indianapolis, is primarily responsible for the overall operation of STANFINS. In addition to this responsibility, the PMO helps to ensure the development and implementation of policies related to STANFINS and corresponding accounting operations; the administration and operation of the system in accordance with DoD security and operational requirements, as well as decision making regarding the strategic direction of future system operations, including anticipated fixes and enhancements, if any; and consideration of eventual STANFINS replacement alternatives. The PMO is also responsible for the implementation of the STANFINS C&A process in accordance with DITSCAP, DoD's governing policy and detailed instructions for carrying out C&As.

The TSO, headquartered in DFAS-Indianapolis, is responsible for elements of the technical administration of STANFINS and provides multi-tier system support in coordination with other organizations (see paragraph below).

The TSO develops and performs unit and function testing changes to the STANFINS production environment and is responsible for the administration of STANFINS' database configuration and maintenance. TSO is responsible for CICS and TAPS administration and maintenance. Additionally, TSO is responsible for elements of security administration for the STANFINS mainframe resources, including the STANFINS application itself. The TSO carries out its responsibilities for security administration in coordination with the DISA Systems Management Center at the DECC-St. Louis. The TSO carries out its responsibilities for many aspects of system support in coordination with the CDOIM, as well as decentralized DOIM organizations servicing other DFAS sites.

The CDOIM is also located at DFAS-Indianapolis. CDOIM is responsible for the overall management and continuance of the STANFINS batch production cycles, including maintenance of the production job schedule, Job Control Language maintenance, operations monitoring, and the resolution of unintended deviations from the STANFINS production job schedule. CDOIM employs the Control-M scheduling utility to maintain Daily, Weekly, Monthly, or Annual production runs as required. CDOIM is also responsible for providing testing support to the PMO and TSO for STANFINS changes. CDOIM is composed of primary, backup, and alternate analysts, and is also responsible for process scheduling.

Additionally, four decentralized DOIM organizations support the following DFAS field sites: Colorado, Korea, Hawaii, and Japan.

The decentralized DOIM organizations are responsible for the management and continuance of the STANFINS batch production cycles related to the sites that they support.

STANFINS User Organizations

STANFINS is deployed worldwide at DFAS and customer locations, including selected Defense Agencies, DFAS field sites (including Hawaii, San Antonio, Indianapolis, Orlando, Rome, Lawton, Seaside, Denver, and Japan), Army Posts, Camps and Stations (i.e., Fort Riley, Fort Belvoir, Fort Leonard Wood), DeCA, DARPA, and Security Assistance. Additionally, STANFINS supports the accounting activities of other DoD agencies. In all, approximately 36,000 users access STANFINS data.

Communication

Defense Finance and Accounting Service

Pertinent control information is critical to maintain an effective internal control system. Information is identified, captured, and communicated in a form and timetable that enables personnel to carry out their responsibilities in an efficient and effective manner. Management reviews reports containing operational, strategic and financial information that make it possible to monitor and control the organization.

Effective communication also occurs in a broader sense throughout the organization. Management stresses the importance of control responsibilities to personnel. Management accomplishes this through supervision and various communication methods (e-mail, period status meetings, postings, etc.). Personnel understand their duties and roles in the internal control system, as well as how their individual activities relate to the work of others. Management is receptive to employee suggestions on ways to enhance productivity, quality, or other improvements to the current products and services offered by the DFAS/DISA organization.

Defense Information Systems Agency

Computing Services Operations Headquarters develops policies establishing performance standards, operating procedures, operational metrics and reporting, standard capacity and performance reporting, quality assurance and quality control, disaster recovery, strategic planning, and other practices required to guide execution of operations services to meet DISA CSD objectives and customer expectations.

The Central Communications Centers (CCC) are configured with the capability to back up the other CCC and support full network infrastructure operations. The CCC can remotely manage the CSD network infrastructure via a secure out-of-band management network. CCC management responsibilities include the support of routing, switching, Domain Name Services (DNS), Wide Area Networks (WAN) interfaces to DISA Network Services, and network security device operations. The CCC also provides the appropriate event correlation for network and security environments within the data centers and serves as the SMC escalation organization to Wide Area Network management centers Regional Network Operations Service Center (RNOSC) as well as Service/Agency base level management centers.

The CSOD Network Operations is responsible for the up-channel reporting of operations incidents. Categories of incidents have been identified as high impact, high visibility, or high interest requiring detailed reporting to a defined chain of senior management. Specific information requirements have been defined for the incident reports to help ensure completeness, accuracy, and understandability. Standard trouble tickets that provide the basic information must be cleansed to ensure that these informational requirements are met and consolidated into the defined incident reporting format. Centralization of this function from field elements assures consistency and responsiveness to senior management needs.

D. CONTROL OBJECTIVES AND RELATED CONTROL ACTIVITIES

DFAS and DISA control objectives and related controls are included in section III of this report, “Control Objectives, Control Activities, and Tests of Operating Effectiveness,” to eliminate the redundancy that would result from listing them in this section and repeating them in section III. Although the control objectives and related controls are included in section III, they are, nevertheless, integral parts of DFAS and DISA control descriptions.

E. USER ORGANIZATION CONTROL CONSIDERATIONS

The control activities at DFAS and DISA related to STANFINS were designed with the assumption that certain controls would be placed in operation at user organizations. The application of such controls by user organizations is necessary to achieve certain control objectives identified in this report. This section describes some of the controls that should be in operation at user organizations to complement the controls at DFAS and DISA. The following user organization control considerations are not a comprehensive list of all controls that user organizations should employ.

User organizations should have policies and procedures in place to provide reasonable assurance that:

- Hard copy documents (e.g., purchase orders, training orders, and miscellaneous obligation documents) are authorized, accurate, and complete before the user submits them to STANFINS for input and automated processing.
- Authorized individuals input data into STANFINS, enter it accurately and completely, and seek approval from appropriate personnel for transactions that are input.
- Erroneous data are corrected and resubmitted in a timely manner.
- The appropriate users review output for completeness and accuracy.
- STANFINS computer terminals, communication lines, and data outputs are protected from unauthorized access.
- Passwords needed to access STANFINS through computer terminals are protected against unauthorized disclosure and misuse.
- STANFINS' Terminal Area Security Officers (TASO) are notified in a timely manner when employees leave or transfer, supporting TASO ability to cancel system access authority for those individuals.

In addition, some DFAS customers submit data into STANFINS and review and correct their own transactions. In such circumstances, controls should be placed in operation to provide reasonable assurance that only authorized source documents are input; errors are identified timely, reviewed, and corrected; and the correction of errors is appropriately authorized.

Section III: Control Objectives, Control Activities, and Tests of Operating Effectiveness

III. Control Objectives, Control Activities, and Tests of Operating Effectiveness

A. SCOPE LIMITATIONS

The Office of the Inspector General, Department of Defense, specified the control objectives documented in this section. As described in the prior section (section II), STANFINS interfaces with many systems. The controls and tests described in this section of the report are limited to those computer systems, operations, and processes directly related to STANFINS. Controls related to the source and destination systems associated with the STANFINS interfaces are specifically excluded from this review. We did not perform procedures to evaluate the effectiveness of the input, processing, and output controls in these interfacing systems, although we did perform procedures to evaluate STANFINS interface input and output controls. We did not conduct penetration testing on STANFINS because this FISCAM procedure was performed under the *Audit of the Defense Computing Services*, Project Number D2004-D000FC-0191. The fieldwork identified no deficiencies. The Defense Computing Services report will be issued in June 2005.

B. CONTROL DEFICIENCIES

Test procedures disclosed operating effectiveness deficiencies in certain control activities. Where the audit team was able to identify and test additional controls that allowed the control objective to be achieved, we documented such compensating controls and/or circumstances, as well as the description of the operating effectiveness deficiency, in the following matrix. In addition, the audit team identified certain compliance exceptions with DoD IA standards and/or other Federal legislation, criteria, standards, or regulations. Where such exceptions related to the suitability of design and/or operating effectiveness of key controls placed in operation to achieve control objectives, we documented the controls and/or circumstances. In a separate DFAS and DISA management report, the audit team identified compliance exceptions not related to the suitability of design and/or operating effectiveness of key controls intended to achieve control objectives. We have not included these exceptions herein because they do not adversely impact the achievement of the control objectives included in this Service Auditors' Report.

C. CONTROL OBJECTIVES, CONTROL ACTIVITIES, AND TESTS OF OPERATING EFFECTIVENESS

Security Program (SP)

Controls provide reasonable assurance that a security program is established.

Control Description	Tests of Operating Effectiveness	Results of Tests of Operating Effectiveness
Control Activity: SP-1 Risks are periodically assessed.		
<u>DISA</u> DISA DECC completed its Risk Analysis in January 2004. The primary objective of the Risk Analysis was to quantify the level of risk associated with the operating systems. The DISA DECC Risk Analysis is comprised of five parts: threat types, the probability of threat occurring, the potential risks to be realized if the threat occurs, the cost of the threat, and countermeasures. Risk assessments are conducted when a major change occurs or once every three years.	<ul style="list-style-type: none"> Inspected risk assessment policies and the most recent DECC risk assessment to determine whether it was independently performed in compliance with National Institute of Standards and Technology (NIST) 800-30 standards. 	<ul style="list-style-type: none"> No exceptions noted.
<u>DFAS</u> The STANFINS SSAA includes the risk assessment policies and the most recent high-level risk assessment conducted in November 2003, based on MAC III controls. The IA division of TSO performed the MAC III-based risk assessment. The MAC III assessment evaluates existing policies and procedures, and provides a summary of areas of potential risk that relate to STANFINS and safeguards that can be applied to reduce those risks and vulnerabilities.	<ul style="list-style-type: none"> Inspected risk assessment policies and the most recent STANFINS risk assessment to determine whether it was independently performed in compliance with NIST 800-30 standards. 	<ul style="list-style-type: none"> No exceptions noted.
Control Activity: SP-2.1 A security plan is documented and approved.		
<u>DISA</u> DISA DECC documents a security plans that provide basic security guidance for the protection of DECC-St. Louis processing resources. DISA Instruction 630-230-19 provides guidance for the development of security plans for DISA major applications (MA) and GSS. The DECC Director endorses the Executive Summary of the plan.	<ul style="list-style-type: none"> Inspected the DISA DECC security plan to determine whether the security plan was approved and complied with Office of Management and Budget (OMB) Bulletin 90-08 and A-130, as well as NIST 800-18. 	<ul style="list-style-type: none"> No exceptions noted.
<u>DFAS</u> The SSAA Information System Security Policy and Plan sections contain a short description of STANFINS and its	<ul style="list-style-type: none"> Inspected the STANFINS security plan to determine whether the STANFINS security 	<ul style="list-style-type: none"> Exception noted, the description is outdated showing multiple DECCs

Control Description	Tests of Operating Effectiveness	Results of Tests of Operating Effectiveness
systems architecture that summarizes the security objectives for confidentiality, integrity, authenticity, availability, accountability, and economic feasibility of integrated security mechanisms. The policy and plan also addresses control requirements for discretionary access for certain personnel, auditing, service continuity, and personnel screening.	plan was approved and complied with OMB Bulletin 90-08 and A-130, NIST 800-18.	supporting STANFINS. The interface diagram depicts many direct interfaces to STANFINS. Most of the interfaces are to ODS. Also, there is system software that is not described (Control-M, ACF2, VASS and ROSCOE).
Control Activity: SP-2.2 The plan is kept current.		
<u>DISA</u> The DISA DECC security plan is current.	<ul style="list-style-type: none"> Inspected the DISA DECC security plan to determine whether the plan was current. 	<ul style="list-style-type: none"> The most recent DISA DECC security plan is dated January 10, 2004. No exceptions noted.
<u>DFAS</u> The SSAA Authority to Operate (ATO), which in part represents the approval of the security plan as current, is signed by the Director, Information and Technology, a designated approval authority, and is current. It is the responsibility of the STANFINS Program Manager to initiate the STANFINS recertification and reaccreditation at least every three years.	<ul style="list-style-type: none"> Inspected the STANFINS security plan to determine whether the plan was current. 	<ul style="list-style-type: none"> The ATO is signed and dated December 12, 2003. However, subsequent changes to the STANFINS infrastructure have made the System Description in Appendix E of the SSAA – Information System Security Policy outdated. Specifically, description is outdated showing multiple DECCs supporting STANFINS.
Control Activity: SP-3.1 A security management structure has been established.		
<u>DISA</u> <p>The DISA Computing Services Security Handbook defines the responsibilities of the Directors, DISA Security Officer, DISA Designated Approval Authority, DISA Certification Authority, Commander of DISA Computing Services, Chief of the Field Security Officer, DISA Computing Services Security Manager (SM), DISA Computing Services Information Systems Security Officer (ISSO), Network Security Officer (NSO), and TASO.</p> <p>The DISA DECC security plan also outlined the responsibilities of the appointed DISA DECC SM, ISSM, NSO, and Information Systems Security Officers.</p> <p>DISA DECC appoints a primary security official, the ISSM/IA</p>	<ul style="list-style-type: none"> Inquired of Security Branch Chief and inspected an organizational chart to determine whether a person was appointed with specific responsibility for security. Inquired of Security Branch Chief and inspected an organizational chart to determine whether the security appointee was subordinate to STANFINS management or a major user. 	<ul style="list-style-type: none"> No exceptions noted. No exceptions noted.

Control Description	Tests of Operating Effectiveness	Results of Tests of Operating Effectiveness
Manager (IAM)/NSO.	<ul style="list-style-type: none"> Inspected the DISA DECC Security Plan to determine whether it outlined security responsibilities as described in the Control Description. 	<ul style="list-style-type: none"> No exceptions noted.
<u>DFAS</u> The responsibilities of the ISSM at the PMO/TSO, ISSO, and TASOs at DFAS sites are established and documented.	<ul style="list-style-type: none"> Inquired of the ISSO/TASO and inspected an organizational chart to determine whether a person was appointed with specific responsibility for security. Inquired of the ISSO/TASO and inspected an organizational chart to determine whether the security appointee was subordinate to STANFINS management or a major user. Inquired of the ISSO to assess whether owners and users of the system were aware of the security structure. 	<ul style="list-style-type: none"> No exceptions noted. At DFAS San Antonio, DFAS Pacific, DFAS Seaside, DFAS Denver and DFAS Indianapolis, the TASO/security appointee was subordinate to STANFINS management. No exceptions noted.

Control Description	Tests of Operating Effectiveness	Results of Tests of Operating Effectiveness
Control Activity: SP-3.2 Information security responsibilities are clearly assigned.		
<u>DISA</u> DISA DECC appoints a primary security official, the ISSM/IAM/NSO. Additionally, generic job descriptions for IT Specialists in the Security Division and Operations Security Branch document baseline responsibilities for different positions and include an outline of security responsibilities and prohibited activities. DISA DECC position appointment letters include the position descriptions for Security Division personnel who work directly with the STANFINS application. Position appointment letters are used when additional responsibilities are assigned to DECC personnel. The appointment letter details the employees' new roles and duties and the timeframe for which the position will be held.	<ul style="list-style-type: none"> Inquired of Security Branch Chief and inspected the DISA DECC Security Plan to determine whether security responsibilities and expected behaviors were clearly defined and documented. Inspected the position descriptions for key IT positions relevant to STANFINS to determine whether security responsibilities were clearly assigned. 	<ul style="list-style-type: none"> No exceptions noted. No exceptions noted.
<u>DFAS</u> DFAS sites have organizational charts, job descriptions, and standard operating procedures that outline security responsibilities for IT personnel.	<ul style="list-style-type: none"> Inquired of ISSO and inspected documentation, including standard operating procedures and position descriptions for key IT personnel, to determine whether security responsibilities and expected behaviors were clearly defined, assigned, and documented. 	<ul style="list-style-type: none"> At DFAS Rome, job descriptions did not address specific job duties and/or prohibited activities.

Control Description	Tests of Operating Effectiveness	Results of Tests of Operating Effectiveness
Control Activity: SP-3.3 Owners and users are aware of security policies.		
<p><u>DISA</u> DISA DECC follows the guidelines prescribed in DISA Instruction 630-230-19 and the DISA Computing Services Handbook for providing training to DISA DECC staff.</p> <p>DISA DECC personnel must take security awareness training, workplace violence training, and anti-terrorism training before gaining access to any system.</p> <p>Security awareness posters throughout the DECC facility illustrate various security related topics (i.e., viruses, freeware/shareware, unique passwords, etc.).</p> <p>DISA DECC employees must sign a non-disclosure agreement form, which represents an acknowledgement of employees' understanding and acceptance of confidential information disclosure restrictions and requirements.</p>	<ul style="list-style-type: none"> • Inquired of Security Branch Chief as to the procedure to make data owners and system users aware of their security responsibilities. • Inspected the training materials to determine the topics covered. For all employees, inspected training documentation that supported attendance of security awareness training. • Observed the posters throughout the DECC facilities to verify that security topics were communicated. • For IT employees who work with STANFINS, inspected confidentiality/security agreements to determine if they were signed. 	<ul style="list-style-type: none"> • No exceptions noted. • DISA DECC-St. Louis employees had not received annual security awareness training since October 12, 2003. • No exceptions noted • No exceptions noted

Control Description	Tests of Operating Effectiveness	Results of Tests of Operating Effectiveness
<p><u>DFAS</u></p> <p>DFAS sites coordinate new users' security awareness training designed to provide an overview of the security structure at DFAS and other important topics relevant to security. Existing employees must take an annual refresher security awareness training to keep abreast of security related topics.</p> <p>DFAS sites send monthly security highlights via e-mail to keep employees abreast of security related topics.</p> <p>Each new employee fills out attendance listings as evidence that they have completed the security awareness training.</p>	<ul style="list-style-type: none"> • Inquired of ISSO/TASO as to the procedure to make data owners and system users aware of their security responsibilities. Inspected the Information Assurance Training and Certification Plan to determine guidelines for training. • Inspected the training materials to determine whether topics covered addressed security awareness training requirements. • Inquired of PMO, TSO, and DFAS field site management and inspected security awareness training attendance listings and other tools used to track course completion to determine whether employees were receiving security awareness training. 	<ul style="list-style-type: none"> • Four out of ten DFAS field sites (DFAS Pacific, DFAS Japan, DFAS Denver and DFAS San Antonio) had no training plans in place. Two out of ten DFAS field sites (DFAS Orlando and DFAS Columbus) did not track attendance. • There was no DFAS-wide IT Technical Training policy that outlined ongoing training requirements for personnel in IT-related positions. As a result, it was left to each DFAS field site to determine the level of training required for IT-related positions, and attendance was not tracked at every site. • No exceptions noted. • Four out of the ten DFAS field sites had issues with security awareness training attendance: <ul style="list-style-type: none"> • DFAS Columbus did not centrally track who had attended training. • DFAS Rome did not centrally track who had attended said training; training was overdue for 22 of 26 new hires. • At DFAS San Antonio, eight out of 33 current user access forms did not have a training certificate of completion on file. • At DFAS Seaside, 13 out of 31 current user access forms did not complete their annual security awareness training.

Control Description	Tests of Operating Effectiveness	Results of Tests of Operating Effectiveness
Control Activity: SP-3.4 An incident response capability has been implemented.		
<u>DISA</u> The Regional Computer Emergency Response Team has documented incident response procedures (Security Directive #00-1) and uses the DISA Computing Services Handbook for guidance on handling incidents (virus, malicious code, etc.), reporting structure (local and regional), and prioritization of incidents. An Information Assurance Categories listing provides classification guidance for individuals to report information security incidents. DISA DECC-Mechanicsburg has a help desk available for customers to call, e-mail, or otherwise communicate incidents.	<ul style="list-style-type: none"> Inquired of the Network Security Administrator and the Information Assurance Officer and inspected incident response policies and procedures to determine whether the incident response capability was documented as required by NIST 800-61. Inspected the Information Assurance Categories listing to determine whether classification guidance for individuals to report information security incidents was documented. Observed the DISA DECC help desk function to note whether an appropriate help desk function was in place within DISA DECC-Mechanicsburg and DISA DECC-St. Louis. 	<ul style="list-style-type: none"> No exceptions noted. No exceptions noted. No exceptions noted.
<u>DFAS</u> The STANFINS incident response policy is detailed in the SSAA. The incident response plan describes procedures to mitigate security threats to the STANFINS system, types of reportable incidents, and specifies designated staff members responsible for each type of potential incident. Network security violations and internal control weaknesses are reported to the ISSO and password compromises are reported to the TASO. The plan outlines a specified, centralized reporting procedure for reportable security incidents.	<ul style="list-style-type: none"> Inquired of the ISSM and TSO personnel and inspected incident response policies and procedures in the SSAA to determine whether the incident response capability had characteristics required by NIST 800-61. 	<ul style="list-style-type: none"> The incident response plan did not include awareness training for individuals with access to the system that addresses how to use the system's incident response capability.
Control Activity: SP-4.1 Hiring, transfer, termination, and performance policies address security.		
<u>DISA</u> The DISA Computing Services Security Handbook prescribes guidelines addressing personnel security controls and addresses position sensitivity designations, documenting and updating designations, investigation and reinvestigation requirements, and adjudication and clearance procedures. The DISA	<ul style="list-style-type: none"> Inquired of Security Branch Chief to note whether hiring, transfer, termination policies addressed security. Inquired of Security Branch Chief to note the 	<ul style="list-style-type: none"> No exceptions noted. No exceptions noted.

Control Description	Tests of Operating Effectiveness	Results of Tests of Operating Effectiveness
<p>Computing Services Handbook also addresses the termination process for all DISA DECC employees.</p>	<p>background investigation process for new and current employees. Inspected Computing Services Handbook to determine whether it addressed these processes.</p> <ul style="list-style-type: none"> Inspected all IT staff personnel records to determine whether authorized personnel contacted references, performed background checks, and filed appropriate documentation on separated employees. For IT employees who work with STANFINS, inspected confidentiality/security agreements to determine if they were signed. 	<ul style="list-style-type: none"> DISA DECC-St. Louis had three out of eight employees that had separated from the facility without exit records on file, therefore allowing users to potentially retain access to sensitive areas within the computing center. DISA DECC-St. Louis did not possess signed confidentiality/ security agreements for three of 15 employees.
<p><u>DFAS</u></p> <p>Human Resources follows policies and procedures prescribed by the Office of Personnel Management (OPM), and uses DoD guidelines and DFAS regulations as supplementary sources for hiring, performance of background checks, transfer, and termination of employees.</p> <p>All new employees must undergo DFAS New Employee Orientation and complete required security related on-boarding tasks, including a security and safety briefing and Personal Identification Number (PIN) identification for Common Access Cards (CACs). Authorized personnel conduct and document background investigations.</p> <p>Employees must undergo an “Out-Processing” clearance procedure if terminated or transferred from DFAS sites. A form is completed identifying application access privileges that need to be deleted. Also, the ISSO must sign and complete a security access worksheet. This worksheet details the type of access the employee was granted, date system access was approved, security initials, and date terminated.</p>	<ul style="list-style-type: none"> Inquired of ISSO and Recruitment Chief to note whether hiring, transfer, and termination policies and procedures addressed security. Inspected the OPM guidance that Human Resources follows to determine whether procedures addressed OPM policies and procedures. Inspected materials used for New Employee Orientation and Out-Processing to determine whether security content was included. Inquired of ISSO and Recruitment Chief to determine the background investigation process for new and current employees. Inspected IT personnel records to determine whether references were contacted and background checks performed and/or confidentiality agreements were complete. For recently terminated employees, inspected 	<ul style="list-style-type: none"> No exceptions noted. No exceptions noted. Positions at DFAS-Rome are SF-85P Non-Critical Sensitive and new hires did not sign a security or confidentiality agreement. DFAS-Denver did not maintain information supporting the level of background investigation for any of the 15 accounting and IT personnel. DFAS San Antonio did not maintain

Control Description	Tests of Operating Effectiveness	Results of Tests of Operating Effectiveness
	the corresponding Out-Processing documents to determine whether they were completed.	signed Out-Processing documents for all separated employees.
Control Activity: SP-4.2 Employees have adequate training and expertise.		
<u>DISA</u> DISA DECC has implemented “Certification Program for System Administrators” and “Information Systems Service Providers.” The program, dated August 2002, and the DISA Computing Services Handbook, outline several different certification courses that system administrators should take depending on their designated level. IT personnel are allowed to take technical training classes outside of DISA DECC programs as long as the training program is within budget and is justifiable based on job responsibility/position requirements. Personnel maintain training documentation in individual personnel files.	<ul style="list-style-type: none"> Inquired of the Security Branch Chief and inspected the DISA Computing Services Handbook to determine whether a program was in place to provide adequate training to IT personnel. For IT employees, inspected training records to determine courses taken. 	<ul style="list-style-type: none"> No exceptions noted. DISA DECC-St. Louis had one IT employee that did not receive any IT technical training since entering the position (ACF2 Administrator) in December 2003. DISA DECC-St. Louis had not provided employees annual security awareness training since October 12, 2003.
<u>DFAS</u> DFAS uses DoD directive 8500.1 and Instruction 8500.2 – “Information Assurance Training, Certification, and Workforce Management” for training direction. This guidance describes training requirements for system administrators, as well as Program Managers, ISSMs, ISSOs, and TASOs, and addresses the information assurance training requirements for end-users. Personnel maintain training documentation in individual personnel files, supporting both technical training and security awareness training.	<ul style="list-style-type: none"> Inquired of Assistant Network Security Officer, the ISSM, and PMO and TSO personnel to determine the structure of the training program in place. Inspected DoD directive 8500.1, 8500.2, and the IT Technical Training Program to determine whether a program was in place to provide adequate training to IT personnel. 	<ul style="list-style-type: none"> Of the ten DFAS field sites, DFAS-Pacific, DFAS-Japan, DFAS-Denver and DFAS-San Antonio did not have training plans in place. Of the ten DFAS field sites tested, DFAS-Orlando and DFAS-Columbus did not track training attendance. There was no DFAS-wide IT Technical Training policy that outlined ongoing training requirements for personnel in IT-related positions. As a result, each DFAS field site determined the level of training required for IT-related positions, and attendance was not tracked at every site.

Control Description	Tests of Operating Effectiveness	Results of Tests of Operating Effectiveness
	<ul style="list-style-type: none"> Inspected job descriptions for IT personnel and compared it with their educational backgrounds and experiences to determine adequacy. For IT personnel, inspected technical training records to determine completion of courses. 	<ul style="list-style-type: none"> Of the ten DFAS field sites, DFAS San Antonio did not have an annual technical IT training program in place for system administrators. No exceptions noted. Of the ten DFAS field sites (DFAS-Pacific) a TASO had not taken training for two years and another TASO had not taken training for three years. Of the ten sites visited, DFAS-San Antonio, DFAS-Orlando and DFAS-Columbus did not track completion of IT technical training.
Control Activity: SP-5.1 Management periodically assesses the appropriateness of security policies and compliance with them		
<u>DISA</u> DISA's FSO performs SRRs as a part of its IA review and certification and accreditation process once every two years. The SRR is an evaluation against DoD STIGs and DoD guidance and policies. Recertification must occur if there are any major upgrades, changes, or breaches. Also, DISA DECC-St. Louis performs similar tests (using the same evaluation criteria) on a more frequent basis to monitor compliance. Additionally, DISA's FSO conducts annual penetration testing. DISA DECC-St. Louis conducts penetration testing approximately every two months, or more frequently if necessary, to ensure that DECC systems information assurance capabilities continue to provide adequate assurance against constantly evolving threats.	<ul style="list-style-type: none"> Inquired of Security Branch Chief to note the methods used to assess compliance with security policy. Inspected the DISA DECC-St. Louis mainframe and network platform STIGs to determine whether security configuration requirements were documented. Inspected the network and mainframe platform SRRs to determine whether management assessed compliance with security policies. 	<ul style="list-style-type: none"> No exceptions noted. No exceptions noted. No exceptions noted.
<u>DFAS</u> The PMO prepares a STANFINS-specific Federal Managers'	<ul style="list-style-type: none"> Inquired of the ISSM, PMO and TSO staffs to 	<ul style="list-style-type: none"> No exceptions noted.

Control Description	Tests of Operating Effectiveness	Results of Tests of Operating Effectiveness
<p>Financial Integrity Act (FMFIA) report once a year. DFAS Arlington, Virginia prepares a Federal Information Security Management Act report for all DFAS information systems, including STANFINS.</p> <p>The SSAA, the FMFIA Report of 2004, and the Threat and Vulnerabilities Assessment 2003 document the most recent self-assessments of STANFINS controls.</p> <p>STANFINS must be re-accredited every three years or sooner if the overall security posture of the systems significantly changes.</p>	<p>determine whether they developed processes to assess the appropriateness of security policies.</p> <ul style="list-style-type: none"> Inspected the STANFINS self-assessment of controls located in the SSAA to verify that STANFINS was included in the scope. Inspected the most recent FMFIA reports to determine whether the PMO completed an FMFIA report related to STANFINS. Inspected the signed Authority to Operate to determine whether a C&A was completed in the past three years. 	<ul style="list-style-type: none"> STANFINS was included in the SSAA self-assessment scope. However, the SSAA did not meet all the requirements of DITSCAP and DoD Instruction 8500.2. Specifically, <ul style="list-style-type: none"> Section 3, "System Architectural Description," page 17, did not meet the requirements for a current and comprehensive baseline inventory of all software. Appendix K, "Incident Response Plan, did not adequately address several requirements related to security awareness of the Incident Response Plan. No exceptions noted. No exceptions noted.
<p>Control Activity: SP-5.2 Management ensures that corrective actions are effectively implemented.</p>		
<p><u>DISA</u> DISA DECC maintains a Plan of Action and Milestones (POAM) that tracks all issues identified through SRR reviews including specific weaknesses, resources needed to implement corrective actions, progress in addressing weaknesses, and scheduled completion basis. It is the responsibility of the DISA DECC primary security official to send a status to DISA FSO to update their progress on the POAM issues.</p>	<ul style="list-style-type: none"> Inquired of Security Branch Chief as to the process for recording corrective actions that need to be implemented. Inspected the POAM to determine whether review findings and associated corrective actions were documented. 	<ul style="list-style-type: none"> No exceptions noted. No exceptions noted.

Control Description	Tests of Operating Effectiveness	Results of Tests of Operating Effectiveness
Additionally, summary level results of the most recent SRRs are tracked through resolution in the Vulnerability Management System (VMS).	<ul style="list-style-type: none"> Inspected summary level results of the most recent SRRs in VMS for the ASIMS domains and DECC network to determine whether SRRs were tracked. 	<ul style="list-style-type: none"> No exceptions noted.
<u>DFAS</u> A matrix is used to follow up on the FMFIA Report. The matrix identifies potential weaknesses. A testing matrix identifies control standards, evaluation methodology, and evaluation results for management controls.	<ul style="list-style-type: none"> Inspected the FMFIA Report matrix to determine whether review findings and associated corrective actions were documented 	<ul style="list-style-type: none"> No exceptions noted.

Access Control (AC) – Logical Security

Controls provide reasonable assurance that logical access to the STANFINS application, as well as the underlying operating systems and network resources, are restricted to properly authorized individuals.

Control Description	Tests of Operating Effectiveness	Results of Tests of Operating Effectiveness
<i>Control Activity:</i> AC-1.1 Resource classifications and related criteria have been established.		
<u>DFAS</u> DFAS has documented and communicated Service-wide and STANFINS-related policies, procedures, and guidance addressing resource classification and associated security requirements as a part of the STANFINS SSAA. The SSAA identifies STANFINS as a MAC III system and documents the resources required to preserve the confidentiality, reliability, and availability of STANFINS data. Additionally, the SSAA contains an evaluation of existing policies and procedures, vulnerabilities, and weaknesses and data flows. It also provides a summary of areas of potential risk that relate to STANFINS recommendations and safeguards that can be applied to reduce risks and vulnerabilities exploitable by threat sources.	<ul style="list-style-type: none"> Inquired of TSO and PMO management and inspected the application security plans to determine whether a specific level of control (classification) was assigned to systems and resources based on the degree of the need to preserve confidentiality, reliability, and availability.. 	<ul style="list-style-type: none"> No exceptions noted.
<i>Control Activity:</i> AC-1.2 Owners have classified resources.		
<u>DFAS</u> DFAS has documented and communicated Service-wide and STANFINS-related policies, procedures, and guidance addressing resource classification and associated security requirements as a part of the STANFINS SSAA. The SSAA identifies STANFINS as a MAC III system and documents the resources required to preserve the confidentiality, reliability, and availability of STANFINS data. Additionally, the SSAA contains an evaluation of existing policies and procedures, vulnerabilities, weaknesses and data flows. It also provides a summary of areas of potential risk that relate to STANFINS, as well as recommendations and safeguards that can be applied to reduce risks and vulnerabilities.	<ul style="list-style-type: none"> Inquired of TSO and STANFINS PMO management and inspected documentation to determine whether system owners had classified resources based on criteria and whether the classification was in accordance with the specific risk assessment. Inspected the risk assessment for STANFINS and the applicable GSS to determine whether a risk assessment was conducted based on NIST 800-30 and DoD Instruction 8500.2. 	<ul style="list-style-type: none"> No exceptions noted.
<i>Control Activity:</i> AC-2.1 Resource owners have identified authorized users and their access authorized.		

Control Description	Tests of Operating Effectiveness	Results of Tests of Operating Effectiveness
<p><u>DISA</u> The DISA Computing Services Security Handbook details granting access to system resources.</p> <p>Users at the DISA DECC-St. Louis have access to STANFINS application production files and data as necessary to support system operation and respond to customer requests. DECC users also have access to the mainframe GSS where the application resides. The DECC is responsible for creating and maintaining DECC user accounts, as well as DFAS ISSO and TASO accounts at customer sites. The local ISSO/TASO is responsible for creating and maintaining user accounts at customer sites.</p> <p>Users at the DECC (the majority of which are system software maintenance personnel) requiring access to the mainframe environment complete a form DD 2875 "System Authorization Access Request," used for initial access requests, as well as for changes to an account. An authorized supervisor must sign this form indicating approval of the access. Users must possess a security clearance commensurate with the classification level of the system in order to obtain access. Passwords are communicated to users via secure means, either in person or via e-mail using separate e-mails to transmit user ID and password.</p> <p>The Remote Access Service (RAS) server connections provide direct dial-in access to the network. DECC users requesting remote access must submit an approved access request form (Form DD 2875). Remote access is granted to users with a valid need, which must be approved by a supervisor, to access the network remotely. Typically, users are granted remote access in order to respond quickly to emergency situations and resolve problems when not at the DECC facility. After receiving an approved remote access request, the Security Division staff adds the user to the RAS server.</p>	<ul style="list-style-type: none"> • Inspected policies and procedures for granting and monitoring access to STANFINS IT resources. • Inquired of DISA DECC-St. Louis Security Division Branch Chief to determine the process for granting access to STANFINS. • Inspected access control procedures to determine whether the process for granting, monitoring, and removing access to STANFINS followed Federal (NIST SP 800-26 – Logical Access) and DoD guidance (DoD Instruction 8500.2 – Remote Access, Access Procedures, Access Control Policies, Contractor and Foreign Nationals Access, Comprehensive Account Management, Least Privilege Procedures, Classified Data Protection). • Inspected access forms for a random sample of users of STANFINS (at the application and network level) to determine whether management authorized access. 	<ul style="list-style-type: none"> • No exceptions noted. • No exceptions noted. • No exceptions noted. • At DISA DECC-St. Louis, we selected 42 users out of 1441 and requested their user access request form packets. Out of the sample of 42 packets: <ul style="list-style-type: none"> • One user did not have a completed access request form; • Three individuals had at least one access request form without a Security representative's signature certifying that the individual's background checks/security clearances were appropriate; • Six individuals had at least one access request form where the user acknowledgement portion was not signed.

Control Description	Tests of Operating Effectiveness	Results of Tests of Operating Effectiveness
	<ul style="list-style-type: none"> • Inquired of DISA DECC-St. Louis Security Division Branch Chief regarding policies and procedures for recertifying users access in STANFINS. • Obtained and inspected the access control listing (ACL) for STANFINS to determine whether terminated employees had access. • Inspected ACL to determine whether duplicate accounts existed. • Inspected an ACL of remote users to determine whether management limited, documented, and approved access. 	<ul style="list-style-type: none"> • DISA DECC-St. Louis did not have a process for recertifying user access to STANFINS. • Two separated employees retained access to one or more of the domains where STANFINS resides. • No duplicate accounts were identified. However, three accounts on the Far East domain had no user name associated with the ACF2 ID (ACID). • Remote access to the DISA DECC-St. Louis mainframes via telnet was not restricted and not secured via encryption.
<p><u>DFAS</u> The Procedures for ASIMS Access Controls details policies on security access responsibilities and the process to grant user access to STANFINS. DFAS uses user access forms to document the establishment, modification, deletion, or suspension of access to STANFINS IT resources, including the STANFINS application and the ELAN that DFAS administrative and field sites use to gain access to STANFINS.</p> <p>The ELAN administrator, prior to establishing a network user ID and password, must approve and sign the access request form. For some sites, a separate security group approves the form via signature.</p> <p>Users must have a TAPS account in order to access the STANFINS application. The local TASO/ISSO is responsible for security administration, including the assignment of TAPS accounts. The ISSO creates user accounts for TAPS/STANFINS through a tool called VASS. For the</p>	<ul style="list-style-type: none"> • Inspected DFAS policies and procedures to determine whether guidance was established to outline ELAN administrator security responsibilities. • Inspected access control procedures to determine whether the process for granting, monitoring, and removing access to STANFINS and GSS followed Federal (NIST SP 800-26 – Logical Access) and DoD 	<ul style="list-style-type: none"> • Of the four DFAS sites tested, DFAS-Indianapolis (PMO and TSO), DFAS-Pacific, DFAS-Japan and DFAS-Rome stated that there was no DFAS service-wide policy or guidance document outlining local ELAN administrator security responsibilities versus those of centralized groups responsible for the administration/ monitoring of DFAS-wide network security. • DFAS field sites did not have the technical knowledge to generate STANFINS and TAPS user access lists directly from the security system. As a result, of the ten DFAS field sites, DFAS-Rome, DFAS-

Control Description	Tests of Operating Effectiveness	Results of Tests of Operating Effectiveness
<p>majority of DFAS field sites, Microsoft Excel spreadsheet, Access database, or other manual means of tracking are used to identify STANFINS/TAPS users, TAPS mode profiles, and assigned TAPS modes. At DFAS-Orlando and DFAS-Japan, TASOs/ISSOs generate ACF2-native listings to identify and track who has access to TAPS and STANFINS.</p> <p>The DFAS Information System Security Plan (ISSP) provides guidance in conducting monthly recertifications of STANFINS and ELAN accounts. The ISSO is responsible for providing each supervisor with a STANFINS user access list. The supervisor is responsible for validating and authorizing user access.</p> <p>Remote network access is granted to users with a valid need, which must be approved by a supervisor, to access the network remotely via Defense Internet Service Provider (DISP) accounts.</p>	<p>guidance (DoD Instruction 8500.2 – Remote Access, Access Procedures, Access Control Policies, Contractor and Foreign Nationals Access, Comprehensive Account Management, Least Privilege Procedures, Classified Data Protection).</p> <ul style="list-style-type: none"> Inspected access forms for a random sample of users of STANFINS (at the application and network level) to determine whether management authorized access. 	<p>Denver, DFAS-San Antonio, DFAS-Lawton, DFAS-Columbus, DFAS-Indianapolis and DFAS-Pacific, DFAS-Seaside DFAS field sites could not:</p> <ul style="list-style-type: none"> Identify all TAPS modes (access privileges) assigned to users; Determine whether users had inappropriate access to TAPS modes, based on job responsibilities; and Determine whether manually derived and maintained access control lists accurately reflected the user population. <ul style="list-style-type: none"> Of the ten DFAS field sites, nine field sites (DFAS-Rome, DFAS-Denver, DFAS-Lawton, DFAS-San Antonio, DFAS-Columbus, DFAS-Seaside, DFAS-Indianapolis, DFAS-Pacific and DFAS-Japan) either used locally developed or had not documented procedures for granting, approving, monitoring, recertifying, and removing user access to STANFINS and the ELAN. Six of ten DFAS user sites did not have complete or existing authorizations for STANFINS users: <ul style="list-style-type: none"> DFAS-Denver: <ul style="list-style-type: none"> 18 STANFINS user access forms did not have an ELAN Account Request Form on file. DFAS-Pacific: <ul style="list-style-type: none"> Justification for STANFINS user access was pre-populated on user access forms by the TASOs and may not support actual needs.

Control Description	Tests of Operating Effectiveness	Results of Tests of Operating Effectiveness
		<ul style="list-style-type: none"> • The functional data owner's signature was missing from TAPS user request forms on two of the eight forms inspected. <p>DFAS-Japan:</p> <ul style="list-style-type: none"> • Four out of 31 ELAN access request forms that users filled out in 1998 did not have an approval (signature). • Two external ELAN users had not signed user agreements. • Seven out of 53 DD 2875/DISA 41 forms did not contain a business reason for the access request. • One out of 53 DD 2875/DISA 41 forms did not contain a business case that adequately explained the reasoning for the access request. • One out of 26 DISP User Access Request forms could not be found. • Two out of 26 user access forms were not signed by the TASO. • One out of 26 user access forms did not contain a supervisor signature or a business case justification. <p>DFAS-Rome:</p> <ul style="list-style-type: none"> • Three out of 30 user access forms did not have authorization documentation available. • 11 of 29 users with DISP accounts did not have a DISP user access request form with the appropriate approvals and/or justification. Two of these users had STANFINS accounts. <p>DFAS-San Antonio:</p> <ul style="list-style-type: none"> • 32 out of 41 LAN user access forms did not have an access request form on file.

Control Description	Tests of Operating Effectiveness	Results of Tests of Operating Effectiveness
	<ul style="list-style-type: none"> Inquired of DFAS field site ISSOs/TASOs to determine whether DFAS periodically recertified user access levels. 	<p>DFAS-Seaside:</p> <ul style="list-style-type: none"> 68 of 72 access request forms did not include an adequate business reason/justification for the access requested. 46 of 72 access request forms had a pre-populated response that included the type of access the user needed, but did not justify the access. Three out of 31 internal LAN users access forms did not have the functional data owner's signature. 14 of 31 internal LAN user access forms did not have the original user access request form used to create their account. Four of 31 internal user access request forms were not signed by the information security officer. There was no evidence of LAN access request forms or DISP user access request forms being used prior to February 10, 2005. <ul style="list-style-type: none"> DFAS field sites did not have the technical knowledge to generate STANFINS and TAPS user access lists directly from the security system. At eight out of ten DFAS field sites (DFAS-Rome, DFAS-Denver, DFAS-Lawton, DFAS-San Antonio, DFAS-Columbus, DFAS-Seaside, DFAS-Indianapolis and DFAS-Pacific), the ISSOs/TASOs could not determine whether manually derived and maintained access control lists accurately reflected the user population, and therefore could not accurately perform user recertifications.

Control Description	Tests of Operating Effectiveness	Results of Tests of Operating Effectiveness
	<ul style="list-style-type: none"> Inquired of DFAS ISSOs/TASOs, as well as DFAS field site supervisors, and inspected user access listings to TAPS/STANFINS to determine whether user access was commensurate with job responsibilities. 	<ul style="list-style-type: none"> At DFAS-Japan, DFAS-Lawton, DFAS-San Antonio, DFAS-Pacific, DFAS-Rome and DFAS-Seaside, users had access that was not required by their job responsibilities.
Control Activity: AC-2.2 Emergency and temporary access authorization is controlled.		
DFAS and DISA do not have emergency or temporary access accounts. All user access requests must follow the same access approval procedures. In cases of emergency, the same access forms are used and procedures followed as a normal access request; the only difference is that the request moves through the approval process more quickly.	<ul style="list-style-type: none"> Inquired of DFAS field site ISSOs/TASOs to determine whether the process used to grant emergency and temporary access for STANFINS and/or the GSS was the same as the process for granting regular access. 	<ul style="list-style-type: none"> No exceptions noted.
Control Activity: AC-3.2 Adequate logical access controls have been implemented.		
<u>Common Controls³</u> DoD workstations are Common Access Card (CAC) configured, which means that all employees must enter their CAC card into the CAC card slot of their workstation in order to log on to their workstations. A user's name and ID are associated with each CAC card. When the user exits his or her workstation and removes the CAC card from the slot of the terminal, the workstation automatically locks.	<ul style="list-style-type: none"> At three sites, observed use of CAC cards to determine security practices. 	<ul style="list-style-type: none"> Observed instances of users at DFAS-Indianapolis, DFAS-Orlando and DFAS-Columbus did not remove their CAC cards when leaving their workstations. At DFAS-Indianapolis, DFAS-Orlando and DFAS-Columbus, CAC card security settings did not require entry of a password to "unlock" a workstation screensaver if the CAC card was inserted and after a period of inactivity.
<u>DISA</u> The mainframe access control applications CA-ACF2 and CA-Top Secret protect the STANFINS application and the system software it resides on.	<ul style="list-style-type: none"> Inquired of Security Division Branch Chief and Security Administrators and inspected ACF2 and Top Secret security settings to determine whether the security products were 	<ul style="list-style-type: none"> Minimum password length on each of the five ACF2 ASIMS domains and the one Top Secret ASIMS domain were configured to six characters, while the

³ Common controls are those controls that a DoD organization other than DISA or DFAS implements, and are commonly applied across both DISA and DFAS.

Control Description	Tests of Operating Effectiveness	Results of Tests of Operating Effectiveness
<p>ACF2 and Top Secret mainframe security software enforce discretionary access controls. Also, access to shared and networked file systems outside the mainframe environment is controlled through discretionary access controls enforced through network access privileges.</p> <p>The UML (three letter userid prefix designation for DECC users) Standardization memo establishes user ID rules for DECC users. DECC user IDs identify the user's department, as well as employment status. Additionally, the OS/390 STIG requires a unique ACF2 or Top Secret user ID for every user.</p> <p>Passwords are not displayed as a user logs in to the mainframe. After three invalid log-on attempts, ACF2 automatically terminates the session. For the Top Secret domains, Top Secret suspends the user's account after two invalid log-on attempts.</p> <p>Before authentication, a warning banner is displayed that informs the user that the system is for authorized use only and that activity will be monitored. The terminal session automatically logs the user off after 15 minutes of inactivity and a screen-lock appears after 15 minutes, which requires the user to re-authenticate in order to regain access.</p> <p>Inactive accounts are suspended after 35 days of inactivity and deleted after 90 days of inactivity.</p>	<p>securely configured in accordance with OS/390 STIG guidance to enforce discretionary access controls.</p>	<p>OS/390 STIG required passwords to have a minimum of eight characters.</p> <ul style="list-style-type: none"> • Users on the Top Secret ASIMS domain were not required by the system to use a national character (e.g., \$, @, #) when creating new passwords, as required by the OS/390 STIG. • Users on the ACF2 ASIMS domains could not use their previous four passwords; users should be restricted from using their previous ten passwords as required by the OS/390 STIG. • The Huntsville ASIMS domain had the JOBCK setting set to NOJOBCK. This setting did not require ACF2 to verify whether a user submitting a batch job had been granted the authority to submit batch jobs. • An individual user was assigned to the Master Central Security Administrator (MSCA) account on the Top Secret ASIMS Far East domain. The MSCA designation allows full system access and is not required for individual users. • 26 DECC ACF2 accounts on the ASIMS domains had passwords that did not expire (MAXDAYS not specified). 147 DECC Top Secret accounts on the Far East ASIMS domains had passwords that did not expire (Password Interval = 0).

Control Description	Tests of Operating Effectiveness	Results of Tests of Operating Effectiveness
	<ul style="list-style-type: none"> Inspected the UML Standardization memo to determine whether naming conventions were established for DECC users. Inquired of Security Division Branch Chief and system administrators to determine security procedures for logging on and using the network. Inspected GSS (mainframe) policies and procedures to determine whether security procedures were documented. Inquired of Security Division Branch Chief and inspected procedures to determine whether inactive mainframe user accounts were monitored and removed when not needed. Inspected the Top Secret and ACF2 STANFINS-related domain ACLs to determine whether inactive DECC user IDs were present in the domains. Observed an individual user sign on to the mainframe to determine whether the opening screen provided a warning banner that stated that the system was for authorized use only and that activity was monitored. Observed a PC terminal to determine whether automatic log-off occurred after a preset number of minutes of inactivity. 	<ul style="list-style-type: none"> DECC users had “Write” or “Allocate” access to STANFINS production application datasets on two of five ACF2 ASIMS domains and the Top Secret ASIMS Far East domain. No exceptions noted. No exceptions noted. 451 ACF2 and 108 Top Secret DECC user accounts across the six STANFINS-related ASIMS domains were inactive for over 180 days or had never been used. No exceptions noted. No exceptions noted.
<u>DFAS</u> STANFINS application password and user ID rules are		

Control Description	Tests of Operating Effectiveness	Results of Tests of Operating Effectiveness
<p>configured within the security system software maintained by DISA as described above.</p> <p>DFAS ELAN procedures include requirements that guide ELAN administrators in the conduct of network security administration.</p> <p>During log-in to the ELAN, there is a banner warning users that they are about to log on to a government workstation and that their use will be monitored. This banner automatically appears every time a user accesses any DFAS workstation connected to ELAN.</p>	<ul style="list-style-type: none"> Inspected DFAS policies and procedures to determine whether guidance was established to outline ELAN administrator security responsibilities. Observed an individual user sign on to the network to determine whether the opening screen provided a warning banner that stated that the system was for authorized use only and that activity was monitored. 	<ul style="list-style-type: none"> DFAS-Indianapolis, DFAS-Pacific, DFAS-Japan and DFAS-Rome maintained no DFAS service-wide policy/guidance document outlining local ELAN administrator security responsibilities versus those of centralized groups responsible for the administration/monitoring of DFAS-wide network security. No exceptions noted.

Control Description	Tests of Operating Effectiveness	Results of Tests of Operating Effectiveness
<p>Control Activity: AC-4.1 Audit trails are maintained.</p> <p><u>DISA</u> Mainframe audit log policies are outlined in the OS/390 STIG, Volume 1. The OS/390 STIG requires review of the following audit entries on a daily basis: dataset access violations, resource violations, and program use violations. The OS/390 STIG requires review of the following audit entries on a weekly/monthly basis: failed log-on attempts and security privileges (i.e., changes to special privileges or attributes). Security reports for the six STANFINS-related ASIMS domains (five ACF2 and one Top Secret domain) are available for DISA DECC-Mechanicsburg and DISA DECC-St. Louis to monitor.</p>		
	<ul style="list-style-type: none"> Inquired of security administrators, inspected policy statements related to audit logging, and compared results to audit settings of security software. Inquired to determine whether all changes to security profiles by security managers were automatically logged and periodically reviewed by management independent of the security function. Inquired of security administrators and inspected logs to determine whether unusual activity was investigated. 	<ul style="list-style-type: none"> No audit log was created for the use of sensitive system utilities on the ACF2 domains; thus, DISA DECC-St. Louis could not review program use violations. Top Secret was not consistently configured to generate audit logs for all sensitive utilities; thus, DISA DECC-St. Louis could not review program use violations. Log data of changes to ACF2 and Top Secret security profiles were not consistently maintained and archived on the mainframe across the six ASIMS (one Top Secret, five ACF2) domains. As a result: <ul style="list-style-type: none"> No ACF2 log review evidence existed, to include changes to ACF2 security profiles, or violation logs prior to January 3, 2005. No Top Secret log review evidence existed, to include changes to security profiles, or violation logs. Sufficient contact information did not exist to adequately follow-up on issues identified during review of the logs. The contacts listed on the logs were not the appropriate contacts. DISA DECC-St. Louis and DISA DECC-Mechanicsburg did not maintain or review logs that detailed activities of remote user sessions.

Control Description	Tests of Operating Effectiveness	Results of Tests of Operating Effectiveness
	<ul style="list-style-type: none"> Inquired of systems administrators and inspected the organizational charts to determine whether monitoring personnel were independent. 	<ul style="list-style-type: none"> DISA DECC-St. Louis and DISA DECC-Mechanicsburg did not maintain evidence of review of ACF2 or Top Secret global system options. DISA DECC-St. Louis and DISA DECC-Mechanicsburg did not segregate monitoring responsibilities for ACF2 and Top Secret audit and violation logs from security administration functions.
Control Activity: AC-4.2 Actual or attempted unauthorized, unusual, or sensitive access is monitored.		
<u>DISA</u> DFAS is responsible for monitoring STANFINS application-specific audit logs. DISA DECC-Mechanicsburg reviews audit logs for the five STANFINS-related ACF2 ASIMS domains as required by the OS/390 STIG (except the program use violation logs). DISA DECC-St. Louis reviews audit logs for the one STANFINS-related Top Secret ASIMS domain.	<ul style="list-style-type: none"> Inquired of security administrators and inspected logs to determine whether audit trails were regularly reviewed and whether security violations were investigated and communicated to management. 	<ul style="list-style-type: none"> No audit log was created for the use of sensitive system utilities on the ACF2 domains; thus, DISA DECC-St. Louis could not review program use violations. Top Secret was not consistently configured to generate audit logs for all sensitive utilities; thus, DISA DECC-St. Louis could not review program use violations. Log data of changes to ACF2 and Top Secret security profiles were not consistently maintained and archived on the mainframe across the six ASIMS (one Top Secret, five ACF2) domains. As a result: <ul style="list-style-type: none"> No ACF2 log review evidence existed, to include changes to ACF2 security profiles, or violation logs prior to January 3, 2005. No Top Secret log review evidence existed, to include changes to security profiles, or violation logs. Sufficient contact information did not

Control Description	Tests of Operating Effectiveness	Results of Tests of Operating Effectiveness
		<p>exist to adequately follow-up on issues identified during review of the logs. The contacts listed on the logs were not the appropriate contacts.</p> <ul style="list-style-type: none"> DISA DECC-St. Louis and DISA DECC-Mechanicsburg did not maintain or review logs that detailed activities of remote user sessions. DISA DECC-St. Louis and DISA DECC-Mechanicsburg did not maintain evidence of review of ACF2 or Top Secret global system options.
<p><u>DFAS</u> If a user accumulates three unsuccessful log-ons to ELAN, the user's account is suspended, which requires reset by ELAN Administrator.</p>	<ul style="list-style-type: none"> Inquired of the ELAN Security Administrator regarding the configuration setting related to account lockout based on the accumulation of a predefined number of unsuccessful log-ons. Inquired of DFAS field site ISSO/TASOs and inspected procedures for the tracking of unsuccessful user access log-on attempts to the ELAN. 	<ul style="list-style-type: none"> DFAS-Denver, DFAS-Pacific, DFAS-Indianapolis, DFAS-Japan, DFAS-Lawton, DFAS-Rome, DFAS-San Antonio and DFAS-Seaside did not maintain audit logs for the ELAN access attempts. DFAS-Denver, DFAS-Lawton, DFAS-San Antonio and DFAS-Rome did not maintain documented procedures for tracking unsuccessful user access log-on attempts to the local LAN.
<p>Control Activity: AC-4.3 Suspicious access activity is investigated and appropriate action taken.</p>		
<p><u>DISA</u> DISA DECC-Mechanicsburg implemented an audit log review spreadsheet as of January 3, 2005, which is used to identify activities that warrant follow-up. Audit log review spreadsheets for each domain are made available to senior management via shared network folders. The Security Division Branch Chief will periodically monitor these files to help ensure the logs are monitored and to review trends.</p> <p>DISA DECC-Mechanicsburg relies on the automated security</p>	<ul style="list-style-type: none"> Inquired of management and inspected documentation to determine whether security violations were summarized and reported to senior management. 	<ul style="list-style-type: none"> Log data of changes to ACF2 and Top Secret security profiles were not consistently maintained and archived on the mainframe across the six ASIMS (one Top Secret, five ACF2) domains. As a result: <ul style="list-style-type: none"> No ACF2 log review evidence existed, to include changes to ACF2 security

Control Description	Tests of Operating Effectiveness	Results of Tests of Operating Effectiveness
<p>reporting features of ACF2. ACF2 generates reports from raw System Management Facility (SMF) records based on type of activity (e.g., log-on ID modification, dataset access violation, etc.). Similarly, DISA DECC-St. Louis relies on the automated security reporting features of Top Secret.</p> <p>The OS/390 STIG requires the DECC to review the ACF2 and Top Secret global control options at least quarterly to determine whether any changes were authorized and necessary.</p>		<p>profiles, or violation logs prior to January 3, 2005.</p> <ul style="list-style-type: none"> • No Top Secret log review evidence existed, to include changes to security profiles, or violation logs. • Sufficient contact information did not exist to adequately follow-up on issues identified during review of the logs. The contacts listed on the logs were not the appropriate contacts.

Access Control (AC) – Physical Security

Controls provide reasonable assurance that physical access controls are established to prevent or detect unauthorized access.

Control Description	Tests of Operating Effectiveness	Results of Tests of Operating Effectiveness
Control Activity: AC-3.1 Adequate physical security controls have been implemented – A. Physical safeguards have been established that are commensurate with the risks of physical damage or access.		
<p><u>DISA</u></p> <p>The DISA DECC facility maintains physical access controls around the compound housing the DECC facility. Exterior doors to the building are secured via an electronic badge reader or keyed locks. Additionally, exterior doors are alarmed. Guards located at the entrance of the compound and Federal Protective Services (FPS) monitor the exterior door alarms.</p> <p>Access to the sensitive computer room areas of the DECC is controlled via an electronic badge reader and as well as a scramble pad. Individuals entering the sensitive areas must present an authorized badge at the badge reader and enter a PIN into the scramble pad to gain access. The code to the combination lock is restricted to a limited number of individuals in the Telecommunications Branch and Security Division.</p> <p>Physical access controls at the DECC are designed to always allow an individual to exit any area of the facility. While an individual can exit a sensitive area without presenting a badge to the badge reader, any individual that does not present a valid badge (i.e., a badge with authorized access to the sensitive areas) before exiting through a door will trigger an alarm through the intrusion detection system and access control system. The Central Station Monitors alert these alarms to the Chief of Security, Federal Protective Services, and facility guards.</p> <p>Closed-circuit video cameras monitor exterior fence lines of the compound housing the DECC. General Services</p>	<ul style="list-style-type: none"> Toured the DISA DECC-St. Louis to determine whether the following physical access controls were in place: <ul style="list-style-type: none"> Electronic badge readers/keyed locks secured exterior doors; Exterior doors were alarmed; Guards were located at the entrance of the compound; Electronic badge readers/scramble pads secured sensitive computer room doors and the tape library; Computer room and tape library were physically separate from administrative areas; Closed-circuit video cameras recorded footage to VHS tapes to monitor exterior fence lines, as well as entrances to all sensitive computer room areas; and Personnel positioned computers to eliminate potential viewing by unauthorized persons. Inspected a list of individuals with access to the computer room to determine whether physical access was commensurate with job responsibilities and no terminated employees retained access to the computer room. 	<ul style="list-style-type: none"> No exceptions noted. At DECC St. Louis, seven individuals on the computer room access list could not be identified by the DECC Security Branch Chief as requiring access to sensitive computer room areas. Those individuals were immediately removed from the access list in October 2004.

Control Description	Tests of Operating Effectiveness	Results of Tests of Operating Effectiveness
<p>Administration-contracted guards, as well as the FPS, monitor these cameras. Within the DECC, closed-circuit video cameras monitor the entrances of all sensitive computer room areas. These cameras are not actively monitored; rather, the cameras record to VHS tapes, which can be used in the event of a security related incident.</p> <p>An authorized identification badge and PIN code is required to enter the computer room and tape/media library at all times. The computer room and tape/media library are separated from the administrative areas, and individuals must be granted access specifically to these areas in order to gain access.</p> <p>GSA is responsible for the issuance of physical keys to the DECC Security Division, and the DECC Security Division is responsible for key control within the DECC facility.</p> <p>Personnel position computer monitors to eliminate potential viewing by unauthorized persons.</p> <p>The Information System Security Standard Operating Procedures (SOP) for Laptop Computer Systems establishes rules of behavior for all laptop system users and outlines security responsibilities for laptop users. Laptops can be taken home by employees or are kept in each employee's work area/office within the controlled access DECC facility.</p>	<ul style="list-style-type: none"> • Attempted to access the computer room without a badge or escort to determine whether the electronic badge system controls the door locking mechanism and restricts access to unauthorized individuals. • For a random sample of individuals with access to the computer room, inspected corresponding user access forms to determine whether access was signed (i.e., approved) by an authorizing official. • Inquired of the Security Branch Chief and inspected the Information System Security SOP for Laptop Computer Systems to determine whether policy established rules of behavior for all laptop system users and outlined security responsibilities for laptop users. 	<ul style="list-style-type: none"> • No exceptions noted. • 27 of 41 users sampled did not have a corresponding access form that was signed by an authorizing official. • No exceptions noted.
Control Activity:		
AC-3.1 Adequate physical security controls have been implemented – B. Visitors are controlled.		
<p><u>DISA</u></p> <p>DECC facility physical access points are controlled by card access and intrusion detection systems at all times. Visitors to the compound must be on an approved visitors listing, which identifies the arrival and expected departure dates for visitors. The guards verify that everyone entering the compound has an authorized form of DoD identification (i.e., CAC card, DISA DECC badge, etc.). Visitors to the compound must provide a valid government-issued identification to be on an approved visitors listing. The Homeland Security Threat Advisory Levels determine how securely a visitor is escorted. Visitor</p>	<ul style="list-style-type: none"> • Inspected the DISA DECC-St. Louis Facility and Building Access Procedures to determine whether visitor processing procedures were documented. • Inquired of DECC Security Branch Chief and guards and observed visitor processing procedures. Walked through the visitor processing procedure during entrance into and exit out of the compound. 	<ul style="list-style-type: none"> • No exceptions noted. • No exceptions noted.

Control Description	Tests of Operating Effectiveness	Results of Tests of Operating Effectiveness
vehicles are inspected for hazardous materials and visitor entry logs are present for all sensitive computer room areas at the DECC.	<ul style="list-style-type: none"> Observed the entry logs for the DISA DECC-St. Louis facility to determine whether visitor access was recorded. 	<ul style="list-style-type: none"> No exceptions noted.

Access Control (AC) and System Software (SS) – Computer Operations

Controls provide reasonable assurance that computer processing occurs in accordance with the documented processing schedule, and schedule deviations are identified and appropriately addressed in a timely manner.

Control Description	Tests of Operating Effectiveness	Results of Tests of Operating Effectiveness
<i>Control Activity:</i> The production scheduling function is adequately separated from other data center functions, such as system software maintenance, logical security, and database administration.		
DISA DECC-St. Louis is responsible for the configuration and access administration of Control-M production scheduling software, as well as other data center functions. The DFAS CDOIM is primarily responsible for the overall management and continuance of the STANFINS batch production cycles, including maintenance of the production job schedule, Job Control Language maintenance, operations monitoring, and the resolution of unintended deviations from the STANFINS production job schedule and ABENDS. Additionally, the decentralized DOIM organizations are primarily responsible for the management and continuance of the STANFINS batch production cycles related to the sites that they support. The DOIM and CDOIM organizations fall under the TSO within DFAS, a separate DoD component from DISA.	<ul style="list-style-type: none"> Inquired of CDOIM/DOIM IT Supervisors and IT Specialists and inspected the CDOIM Operations Management Plan and organizational charts/position descriptions to determine whether the Production Scheduling group was appropriately segregated from other operations groups. 	<ul style="list-style-type: none"> No exceptions noted.
<i>Control Activity:</i> Production scheduling software (Control-M) has been configured securely and provides adequate logical access controls.		
<u>DISA</u> DISA DECC-St. Louis is responsible for the configuration and access administration of Control-M production scheduling software. Control-M has been configured to provide security over the ability to issue operator commands and modify jobs in the queue and individual jobs and schedules.	<ul style="list-style-type: none"> Inspected access listings and security settings to the Control-M scheduling utility to determine whether utility was configured securely. 	<ul style="list-style-type: none"> DISA DECC-St. Louis user access to the Job Status Screen and History Jobs files was excessive based on segregation of duties principles.

Control Description	Tests of Operating Effectiveness	Results of Tests of Operating Effectiveness
Control Activity: Control-M operating procedures and processing schedules are documented and available to operators.		
<u>DFAS</u> All Control-M procedure documentation is available to any member of the CDOIM/DOIMS. The Job Analyzer Utility Manual covers topics including logic, preparations, installation, Job Control Language (JCL) parameters, and analyzing a single job. The User Manual covers topics including rule definition facility, implementation considerations, job production parameters, Control-M Event Manager, and the reporting facility.	<ul style="list-style-type: none"> Inquired of the IT Supervisor and IT Specialists and inspected manuals to determine whether processes were documented and available. 	<ul style="list-style-type: none"> At the DOIM site located in Denver: <ul style="list-style-type: none"> Denver DOIM Management did not develop and implement Control-M standards and procedures to aid personnel in the use of this application. The process for documenting the job schedule changes and any issues during processing was informal. As a result, no documentation existed for these processes. Management did not document a description of STANFINS production jobs; description of ABEND codes; and escalation, recovery, and restart procedures.
Control Activity: Procedures for requesting, approving, and implementing changes to the production schedule are documented and in place.		
<u>DFAS</u> The procedures for scheduling are documented in the CDOIM Operations Management Plan and DOIM SOPs. Each month, the field sites e-mail the CDOIM/DOIM a monthly calendar with all scheduled releases. The CDOIM/DOIM IT Specialist logs into Control-M using a unique user ID and password and accesses the calendar function within Control-M. The IT Specialist then manually enters each of the scheduled releases on the appropriate day(s) of the month, which is determined by the calendar. Control-M then reads and releases each schedule accordingly.	<ul style="list-style-type: none"> Inspected CDOIM Operations Management Plan to determine whether management documented scheduling procedures. Inquired of IT Supervisor and IT Specialist to determine how they received, documented, approved, and tracked schedule change requests through completion/resolution. 	<ul style="list-style-type: none"> No exceptions noted. At all three CDOIM/DOIM sites visited, documentation of schedule requests was not maintained.

Control Description	Tests of Operating Effectiveness	Results of Tests of Operating Effectiveness
Control Activity: Audit trails of production job processing are generated and maintained.		
<p>Control-M records the date and time, user ID and disposition code, and job execution message regarding the completion of production jobs to audit trails.</p> <p>Color-coding facilitates the identification of production jobs that finished in a state of error. Audit trails are generated real-time during the execution of the production schedule and are available for review after-the-fact.</p> <p>Control-M produces a log that identifies that an individual has made a schedule change and the user ID of the person who made the change. Control-M has the ability to filter data to identify deleted schedules and the user who performed the deletion.</p>	<ul style="list-style-type: none"> Inquired of IT Supervisor and Specialist and inspected the settings page to determine the settings applied for recording audit records in SysLog. Inspected a screen print of the Control-M History log to determine whether management documented audit trails of production schedule/job completion. 	<ul style="list-style-type: none"> At the DOIM located in Denver, personnel were unaware of automated logging features in Control-M, stating there was no automated audit logging process for STANFINS job scheduling and processing. At the DOIM located in Denver, personnel were unaware of automated logging features in Control-M, stating there was no automated audit logging process for STANFINS job scheduling and processing.
Control Activity: Realized production issues that cause deviations from the predefined production-processing schedule are identified, documented, and tracked to their resolution. Procedures outline steps for recovery from production issues, and escalation listings/contact information is documented and available to personnel.		
<p><u>DISA</u> DISA DECC-St. Louis and DISA DECC-Mechanicsburg share responsibility for monitoring production processing with DFAS. When an operator at DECC identifies an abnormal job termination ABEND, he/she creates a REMEDY system ticket to track the issue and contacts an appropriate DFAS POC for resolution. Contact lists/escalation procedures document POCs to be called in the event of unresolved ABEND. DISA DECC maintains historical REMEDY tickets as a resource for identifying and resolving production-processing problems. Once the operator alerts DFAS of the issue, DFAS is responsible for identifying a method of resolution and ensuring the problem is resolved.</p>	<ul style="list-style-type: none"> Inquired with Technical Support Branch (TSB) personnel to determine whether a process for identifying, documenting, and tracking production schedule deviations was developed. Inspected the listing of appropriate DFAS points of contact to determine if contact information was documented. For production issues since July 2004, inspected the corresponding REMEDY tickets to determine if they were tracked to completion. 	<ul style="list-style-type: none"> No exceptions noted. No exceptions noted. No exceptions noted.
<p><u>DFAS</u> DISA DECC-St. Louis and DISA DECC-Mechanicsburg share</p>	<ul style="list-style-type: none"> Inquired with Computer/Electronic Data 	<ul style="list-style-type: none"> At the DOIM site located in Denver:

Control Description	Tests of Operating Effectiveness	Results of Tests of Operating Effectiveness
<p>responsibility for monitoring production processing with DFAS.</p> <p>Once DFAS is alerted of the issue, DFAS is responsible for identifying a method of resolution and ensuring the problem is resolved.</p> <p>Some DOIM sites have standard operating procedures to address production job ABENDS and escalation procedures. Processing is monitored real-time and any issues are immediately identified and addressed. When a job encounters an ABEND, the screen turns red and processing stops until an operator corrects the error and restarts the job.</p> <p>Escalation procedures provide detailed instruction on handling ABENDS and identify points of contact.</p> <p>In some cases, Internal Trouble Reports are created when STANFINS processes ABENDS. When an Internal Trouble Report is created, an approval must accompany the change made to fix the processing issue.</p>	<p>Processing (EDP) Specialist to determine whether a process for identifying, documenting, and tracking production schedule deviations was developed. Inspected procedures to determine whether the process was documented and whether a point of contact list was available for reference when problem escalation was necessary.</p> <ul style="list-style-type: none"> Inspected procedures used for production processing and documentation used to track deviations from the predefined production-processing schedule. For production issues since July 2004, inspected the corresponding REMEDY tickets to determine if they were tracked to completion. 	<ul style="list-style-type: none"> Denver DOIM Management did not develop and implement Control-M standards and procedures to aid personnel in the use of this application. The process for documenting the job schedule changes and any issues during processing was informal. As a result, no documentation existed for these processes. Management did not document a description of STANFINS production jobs, description of ABEND codes, and escalation, recovery and restart procedures. <ul style="list-style-type: none"> At the DOIM site located in Denver: <ul style="list-style-type: none"> Denver DOIM Management did not develop and implement Control-M standards and procedures to aid personnel in the use of this application. The process for documenting the job schedule changes and any issues during processing was informal. As a result, no documentation existed for these processes. Management did not document a description of STANFINS production jobs, description of ABEND codes, and escalation, recovery and restart procedures. No exceptions noted.

Change Control (CC)

Controls provide reasonable assurance that program (coding) changes to the STANFINS application are authorized, documented, tested, approved, and properly implemented.

Control Description	Tests of Operating Effectiveness	Results of Tests of Operating Effectiveness
Control Activity: CC-1.1 A system development life cycle methodology (SDLC) has been implemented.		
<u>DFAS</u> The Software Configuration Management Plan (SCMP) dated March 6, 2003 outlines responsibilities, requirements, and procedures related to application development and configuration control. The TSO-Indianapolis Design Specification (DS) Procedure document details procedures, standards, and requirements regarding STANFINS program design. The DFAS STANFINS Software Quality Assurance Plan (SQAP) dated August 2002, details the STANFINS testing requirements, roles, and requirements. The Organization Standard Software Process (OSSP) details the Software Life Cycle and the overview of OSSP Phases and Tasks. The SSAA includes listings of the hosting GSS, hosted Automated Information System (AIS) applications, interconnected outsourced IT-based processes, and interconnected IT platforms.	<ul style="list-style-type: none">• Inspected the Software Configuration Plan, the TSO-Indianapolis DS Procedure, the DFAS STANFINS SQAP, and the OSSP to determine whether a system development life cycle was developed and documented.• Inquired of change management staff to determine whether staff involved with developing and testing software were familiar with the use of the SDLC methodology.• Inspected the SSAA to determine whether it provided a structured approach consistent with generally accepted concepts and practices.	<ul style="list-style-type: none">• No exceptions noted.• No exceptions noted.• No exception noted.

Control Description	Tests of Operating Effectiveness	Results of Tests of Operating Effectiveness
Control Activity: CC-1.2 Authorizations for software modifications are documented and maintained.		
<p><u>DFAS</u></p> <p>STANFINS software changes, with the potential exception of changes required to accommodate interfacing systems, must be accompanied by a completed System Change Request (SCR) form. The SCR must be filled out and approved by the System Owner before the change is tested and migrated to production.</p> <p>Prior to testing, each SCR requires a documented Test Condition Requirements (TCR) form to be filled out including a sign-off documenting the STANFINS PMO Functional group's approval. Testing is performed using production data in a test environment</p> <p>Once the TCR is authorized, the PMO Functional group sends an e-mail to TSO regarding the change release. A checklist is used to determine that all appropriate steps have been taken prior to ship. DECC is contacted to determine that they are ready to receive, and have received, the release.</p>	<ul style="list-style-type: none"> Inspected supporting authorization and testing documentation for STANFINS changes applied during the examination period to determine whether documentation was prepared in accordance with DoD Instruction 8500.2. 	<ul style="list-style-type: none"> Documentation of testing and authorizations related to the development and implementation of STANFINS application changes was inconsistently generated and maintained. These inconsistencies included: <ul style="list-style-type: none"> SCRs were generally not created if the Change Control Board knew that the request would not be authorized. All Change Control Board meetings were informal, held as needed, and most communication regarding proposed changes was discussed verbally (not documented). Of 15 SCRs and TCRs generated October 2, 2002 through October 2004, only three had e-mail documentation to support the change. Of 12 FY 2004 SCRs, only three copies of e-mails notifying the DFAS field sites of changes were maintained.
Control Activity: CC-2.1 Changes are controlled as programs progress through testing to final approval.		
<p><u>DFAS</u></p> <p>STANFINS currently operates in a "maintenance mode," which means that only emergency maintenance changes are applied. Emergency maintenance changes are those software changes required to maintain compliance with applicable Federal statutes and regulations.</p> <p>STANFINS software changes, with the potential exception of changes required to accommodate interfacing systems, must be accompanied by a completed SCR form. The SCR must be filled out and approved by the System Owner before the change is tested and migrated to production.</p>	<ul style="list-style-type: none"> Inspected supporting authorization and testing documentation for STANFINS changes applied during the examination period to determine whether documentation was prepared in accordance with DoD Instruction 8500.2. 	<ul style="list-style-type: none"> Documentation of testing and authorizations related to the development and implementation of STANFINS application changes were inconsistently generated and maintained. These inconsistencies included: <ul style="list-style-type: none"> SCRs were generally not created if the Change Control Board knew that the request would not be authorized. All Change Control Board meetings were informal, held as needed, and

Control Description	Tests of Operating Effectiveness	Results of Tests of Operating Effectiveness
<p>Prior to testing, each SCR requires a documented TCR form to be filled out, including a sign-off documenting the STANFINS PMO Functional group's approval. Testing is performed using production data in a test environment</p> <p>Once the TCR is authorized, the PMO Functional group sends an e-mail to TSO regarding the change release. A checklist is used to determine that all appropriate steps have been taken prior to packaging the software change for DECC implementation. DECC is contacted to determine that they are ready to receive, and have received, the release.</p>	<ul style="list-style-type: none"> Performed inquiry of the PMO Accountant and Lead Specialist to verify the process used to document and authorize changes. 	<p>most communication regarding proposed changes was discussed verbally (not documented).</p> <ul style="list-style-type: none"> Of 15 SCRs and TCRs generated October 2, 2002 through October 2004, only three had e-mail documentation to support the change. Of 12 FY 2004 SCRs, only three copies of e-mails notifying the DFAS field sites of changes were maintained. STANFINS application changes were manually controlled, migrated, and released from the testing environment; however, the documentation was not appropriately maintained as seen in the exception above. Specifically, there was no automated version controls (i.e., a program change version control system) to track changes to STANFINS.
<p><u>DISA</u> The TSB staff in DISA DECC-St. Louis receives final instruction to implement the changes via e-mail from the staff in Indianapolis.</p>	<ul style="list-style-type: none"> Inspected the notification e-mails for a selection of STANFINS changes (all STANFINS changes applied during the examination period were selected) to determine whether such communications between DFAS and the DISA DECC-St. Louis were documented. 	<ul style="list-style-type: none"> No exceptions noted.

Control Description	Tests of Operating Effectiveness	Results of Tests of Operating Effectiveness
<p>Control Activity: CC-2.2 Emergency changes are promptly tested and approved.</p> <p><u>DFAS</u> All changes are considered to be emergency changes and undergo the process documented in Control Activity CC-2.1 <i>Changes are controlled as programs progress through testing to final approval.</i> STANFINS currently operates in a “maintenance mode,” which means that only emergency maintenance changes are applied. Emergency maintenance changes are those software changes required to maintain compliance with applicable Federal statutes and regulations.</p> <p>STANFINS software changes, with the potential exception of changes required to accommodate interfacing systems, must be accompanied by a completed SCR form. The SCR must be filled out and approved by the System Owner before the change is tested and migrated to production.</p> <p>Prior to testing, each SCR requires a documented TCR form to be filled out, including a sign-off documenting the STANFINS PMO Functional group’s approval. Testing is performed using production data in a test environment</p> <p>Once the TCR is authorized, the PMO Functional group sends an e-mail to TSO regarding the change release. A checklist is used to determine that all appropriate steps have been taken prior to packaging the software change for DECC implementation. DECC is contacted to determine that they are ready to receive, and have received, the release.</p>		
	<ul style="list-style-type: none"> Inspected supporting authorization and testing documentation STANFINS changes applied during the examination period to determine whether documentation was prepared in accordance with DoD Instruction 8500.2. Performed inquiry of the PMO Accountant and Lead Specialist to verify the process used to document and authorize changes. 	<ul style="list-style-type: none"> Documentation of testing and authorizations related to the development and implementation of STANFINS application changes were inconsistently generated and maintained. These inconsistencies included: <ul style="list-style-type: none"> SCRs were generally not created if the Change Control Board knew that the request would not be authorized. All Change Control Board meetings were informal, held as needed, and most communication regarding proposed changes was discussed verbally (not documented). Of 15 SCRs and TCRs generated October 2, 2002 through October 2004 (3 in FY 2003 and 12 in FY 2004), only three had e-mail documentation to support the change. Of the 12 FY 2004 SCRs, only three copies of e-mails notifying the DFAS field sites of changes were maintained. STANFINS application changes were manually controlled, migrated, and released from the testing environment; however, the documentation was not appropriately maintained as seen in the exception above. Specifically, there was no automated version controls (i.e., a program change version control system) to track changes to STANFINS.

Control Description	Tests of Operating Effectiveness	Results of Tests of Operating Effectiveness
Control Activity: CC-2.3 Distribution and implementation of new or revised software is controlled.		
<u>DFAS</u> Once the release has been shipped, DISA DECC-St. Louis is responsible for distribution and implementation.	<ul style="list-style-type: none"> Inspected procedures and inquired of an Accountant, IT Specialist, and Lead Technician to obtain an understanding of responsibilities for distribution and implementation of STANFINS application changes. 	<ul style="list-style-type: none"> No exceptions noted.
<u>DISA</u> E-mail communication from DFAS developers denoting items such as the change type, implementation dates, and additional instructions regarding changes are sent directly to the personnel implementing the changes in the TSB. The TSB is responsible for Capacity Management, Operating Systems, Database, and Operations Support at DISA DECC. DISA DECC-St. Louis is responsible for copying all the release data to the production application library. They coordinate with CDOIM/DOIM to implement the production release. The CDOIM/DOIM reconciles the production application library to validate that the DECC completely and accurately copied all the data over to the production directory. The CDOIM/DOIM is responsible for coordinating with all of the appropriate field sites affected by the release. Once a date has been agreed to between the field sites and the CDOIM/DOIM, the CDOIM/DOIM instructs the DECC to release the change on the specified time and date. The DECC releases all changes as specified by the CDOIM/DOIM. Once changes are released, a final notification is sent from the DECC to the CDOIM/DOIM confirming the release.	<ul style="list-style-type: none"> Inspected the notification e-mails for STANFINS changes applied during the examination period to determine whether implementation dates for STANFINS were communicated to personnel implementing the changes in the TSB. Performed inquiry of the PMO Accountant and Lead Specialist to verify the process used to document and authorize changes. 	<ul style="list-style-type: none"> No exceptions noted. No exceptions noted.

Control Description	Tests of Operating Effectiveness	Results of Tests of Operating Effectiveness
Control Activity: CC-3.1 Programs are labeled and inventoried.		
<u>DFAS</u> STANFINS program changes are conducted manually and the IT Specialist is responsible for creating/titling each version change and helping to ensure that each site is using the correct version of STANFINS.	<ul style="list-style-type: none"> Inquired of the Lead Specialist regarding procedures for labeling and inventorying STANFINS application programs. 	<ul style="list-style-type: none"> STANFINS application changes were manually controlled, migrated, and released from the testing environment; however, the documentation was not appropriately maintained. Specifically, there was no automated version controls (i.e., a program change version control system) to track changes to STANFINS. Inconsistencies in documentation included: <ul style="list-style-type: none"> SCRs were generally not created if the Change Control Board knew that the request would not be authorized. All Change Control Board meetings were informal, held as needed, and most communication regarding proposed changes was discussed verbally. Of 15 SCRs and TCRs generated October 2, 2002 through October 2004 (3 in FY 2003 and 12 in FY 2004), only three had e-mail documentation to support the change. Of the 12 FY 2004 SCRs, only three copies of e-mails notifying the DFAS field sites of changes were maintained.
Control Activity: CC-3.2 Access to program libraries is restricted.		
<u>DISA</u> DISA is responsible for administering access to STANFINS production program libraries. DISA administers access based on approved access request forms received from appropriate DFAS points of contact. Additionally, DECC user access to STANFINS production libraries is limited to operation support	<ul style="list-style-type: none"> Inspected policies and procedures on granting and monitoring access to STANFINS IT resources. 	<ul style="list-style-type: none"> No exceptions noted.

Control Description	Tests of Operating Effectiveness	Results of Tests of Operating Effectiveness
<p>staff responsible for responding to customer requests and troubleshooting.</p>	<ul style="list-style-type: none"> • Inquired of DISA DECC-St. Louis Security Division Branch Chief to determine the process for granting access to STANFINS. • Inspected access control procedures to determine whether the process for granting, monitoring, and removing access to STANFINS (including the GSS) followed DoD Instruction 8500.2 <i>Information Assurance Implementation</i> guidance, which requires procedures to address need to know access, security awareness training for users, and verification of a favorable background investigation/ active security clearance. • Inspected access request forms for a random sample of users of STANFINS (at the application and network level) to determine whether management authorized access. • Obtained and inspected the ACL for STANFINS to determine whether terminated employees had access. 	<ul style="list-style-type: none"> • No exceptions noted. • No exceptions noted. • At DISA DECC-St. Louis, we selected 42 users and requested their user access request out of form packets. Out of the sample of 42 packets: <ul style="list-style-type: none"> • One user did not have a completed access request form; • Three individuals had at least one access request form without a Security representative's signature certifying that the individual's background checks/security clearances were appropriate; • Six individuals had at least one access request form where the user acknowledgement portion was not signed. • Two separated employees retained access to one or more of the domains where STANFINS resides.

Control Description	Tests of Operating Effectiveness	Results of Tests of Operating Effectiveness
<p><u>DFAS</u></p> <p>Programmer access to production files is limited. DISA administers access based on approved access request forms received from appropriate DFAS points of contact.</p>	<ul style="list-style-type: none"> Inspected DFAS policies and procedures to determine whether guidance was established to outline ELAN administrator security responsibilities. Inspected access control procedures to determine whether the process for granting, monitoring, and removing access to STANFINS (including the GSS) followed OMB A-130 and DoD guidance. 	<ul style="list-style-type: none"> Of the ten DFAS sites, DFAS-Indianapolis (PMO and TSO), DFAS-Pacific, DFAS-Japan and DFAS-Rome stated that there was no DFAS service-wide policy or guidance document outlining local ELAN administrator security responsibilities versus those of centralized groups responsible for the administration/monitoring of DFAS-wide network security. During testing, DFAS field sites were unable to generate STANFINS and TAPS user access lists directly from the security system. As a result, of the ten DFAS field sites, DFAS-Rome, DFAS-Denver, DFAS-San Antonio, DFAS-Lawton, DFAS-Columbus, DFAS-Indianapolis and DFAS-Pacific, DFAS-Seaside DFAS field sites could not: <ul style="list-style-type: none"> Identify all TAPS modes (access privileges) assigned to users; Determine whether users had inappropriate access to TAPS modes, based on job responsibilities; and Determine whether manually derived and maintained access control lists accurately reflected the user population. Of the ten DFAS field sites, nine field sites (DFAS-Rome, DFAS-Denver, DFAS-Lawton, DFAS-San Antonio, DFAS-Columbus, DFAS-Seaside, DFAS-Indianapolis, DFAS-Pacific and DFAS-Japan) either used locally developed or had

Control Description	Tests of Operating Effectiveness	Results of Tests of Operating Effectiveness
	<ul style="list-style-type: none"> Inspected access forms for a random sample of users of STANFINS (at the application and network level) to determine whether management authorized access. 	<p>not documented procedures for granting, approving, monitoring, recertifying, and removing user access to STANFINS and the ELAN.</p> <ul style="list-style-type: none"> Six of ten DFAS user sites did not have complete or existing authorizations for STANFINS users as follows: <p>DFAS-Denver:</p> <ul style="list-style-type: none"> 18 STANFINS user access forms did not have an ELAN Account Request Form on file. <p>DFAS-Pacific:</p> <ul style="list-style-type: none"> Justification for STANFINS user access was pre-populated on user access forms by the TASOs and may not support actual needs. The functional data owner's signature was missing from TAPS user request forms on two of the eight forms inspected. <p>DFAS-Japan:</p> <ul style="list-style-type: none"> Four out of 31 ELAN access request forms that users filled out in 1998 did not have an approval (signature). Two external ELAN users had not signed user agreements. Seven out of 53 DD 2875/DISA 41 forms did not contain a business reason for the access request. One out of 53 DD 2875/DISA 41 forms did not contain a business case that adequately explained the reason for the access request. One out of 26 Defense Internet Service Provide (DISP) User Access Request forms could not be found. Two out of 26 user access forms were

Control Description	Tests of Operating Effectiveness	Results of Tests of Operating Effectiveness
		<p>not signed by the TASO.</p> <ul style="list-style-type: none"> One out of 26 user access forms did not contain a supervisor signature or a business case justification. <p>DFAS-Rome:</p> <ul style="list-style-type: none"> Three out of 30 user access forms did not have authorization documentation available. 11 of 29 users with DISP accounts did not have a DISP user access request form with the appropriate approvals and/or justification. Two of these users had STANFINS accounts. <p>DFAS-San Antonio:</p> <ul style="list-style-type: none"> 32 out of 41 LAN user access forms did not have an access request form on file. <p>DFAS-Seaside:</p> <ul style="list-style-type: none"> 68 of 72 access request forms did not include an adequate business reason/justification for the access requested. 46 of 72 access request forms had a pre-populated response that included the type of access the user needed, but did not justify the access. Three out of 31 internal LAN user access forms did not have the functional data owner's signature. 14 of 31 internal LAN user access forms did not have the original user access request form used to create their account. Four of 31 internal users' access request forms were not signed by the information security officer. There was no evidence of LAN access request forms or DISP user access

Control Description	Tests of Operating Effectiveness	Results of Tests of Operating Effectiveness
	<ul style="list-style-type: none"> Inquired of DFAS ISSOs/TASOs, as well as DFAS field site supervisors, and inspected user access listings to TAPS/STANFINS to determine whether user access was commensurate with job responsibilities. 	<p>request forms being used prior to February 10, 2005.</p> <ul style="list-style-type: none"> At DFAS-Japan, DFAS-Lawton, DFAS-San Antonio, DFAS-Pacific, DFAS-Rome and DFAS-Seaside, users had access that was not required by their job responsibilities.
Control Activity: CC-3.3 Movement of programs and data among libraries is controlled.		
<u>DISA</u> Production program changes are migrated by DISA DECC-St. Louis personnel. DISA DECC-St. Louis personnel receive changes from authorized points of contact and implement changes in the production environment as directed by DFAS POCs.	<ul style="list-style-type: none"> Inquired of the TSB Chief and inspected policies and procedures regarding movement of STANFINS programs among libraries. 	<ul style="list-style-type: none"> No exceptions noted.
<u>DFAS</u> DFAS has documented a change control process and work flow plan that details how each change is identified, requested, approved, and moved along the appropriate libraries.	<ul style="list-style-type: none"> Inspected a work flow diagram regarding movement of STANFINS programs among libraries. 	<ul style="list-style-type: none"> No exceptions noted.

System Software (SS)

Controls provide reasonable assurance that the implementation of new system and vendor-supplied software and utilities and changes to existing system and vendor-supplied software and utilities are authorized, tested, approved, properly implemented, and appropriately documented.

Control Description	Tests of Operating Effectiveness	Results of Tests of Operating Effectiveness
Control Activity: SS-1.1 Access authorizations are appropriately limited.		
<p><u>DISA</u></p> <p>Policies for restricting access to systems software are detailed in the OS/390 STIG. The document establishes guidelines for restricting access to sensitive system datasets. The network device control policy is detailed in the Network Infrastructure STIG, which outlines access restrictions to network devices, and also details the secure configuration of network devices.</p> <p>The Executive Software Configuration Control Board (ESCCB) uses a Web-based application, the Software Factory, on software package distribution database, to receive all software configuration change requests and then routes them to the appropriate ESCCB staff and board for approval. The Software Factory does not allow access to the software unless the individual is listed on an authorized user listing. The individual must have permissions established within Resource Access Control Facility (RACF) and must also match the authorized user listing of the Software Factory application. Additionally, when the individual accesses the Software Factory, the system is automatically configured to distribute e-mail notifications to designated points of contact at the DISA DECC-Mechanicsburg, DISA DECC-St. Louis, and SSO-Mechanicsburg.</p>	<ul style="list-style-type: none"> Inspected Top Secret and Access Control Facility 2 (ACF2) STANFINS-related domain ACLs to determine whether access to system software datasets and utilities was limited. Inspected the listing of authorized users for Software Factory and RACF at DISA DECC-Mechanicsburg and DISA DECC-St. Louis and inquired of DISA DECC-St. Louis TSB Chief to determine whether user access was commensurate with job responsibilities. 	<ul style="list-style-type: none"> DECC users had “Write” or “Allocate” access to STANFINS production application datasets on two of five ACF2 ASIMS domains and excessive access on the Top Secret ASIMS Far East domain. Access to SYS1 datasets was assigned inconsistently across the ACF2 ASIMS domains. Additionally, access to SYS1 datasets was not based on segregation of duties principles for the ACF2 and Top Secret domains. DISA DECC-St. Louis did not restrict access to sensitive system software utilities on the ACF2 domains via the Protected Program List (PPGM), as required by the OS/390 STIG. For Top Secret, access to sensitive utilities on the Top Secret ASIMS Far East domain was not restricted based on segregation of duties principles. At the DECC-Mechanicsburg, two individuals on the listing no longer required access to the Software Factory. At DECC-St. Louis, users had access to sensitive datasets that were not necessary for their job responsibilities.

Control Description	Tests of Operating Effectiveness	Results of Tests of Operating Effectiveness
Control Activity: SS-2.1 Policies and techniques have been implemented for using and monitoring use of system utilities.		
<u>DISA</u> Mainframe audit log policies are outlined in the OS/390 STIG, Volume 1. The OS/390 STIG requires review of dataset access violations, resource violations, and program use violations on a daily basis and requires review of the failed log-on attempts and security privileges on a weekly/monthly basis. Security reports for the six STANFINS-related ASIMS domains (five ACF2 and one Top Secret domain) are available for DISA DECC-Mechanicsburg and DISA DECC-St. Louis to monitor.	<ul style="list-style-type: none"> Inquired of security administrators and inspected policy statements related to audit logging and compared results to audit settings of security software. 	<ul style="list-style-type: none"> No audit log was created for the use of sensitive system utilities on the ACF2 domains; thus, DISA DECC-St. Louis could not review program use violations. Top Secret was not consistently configured to generate audit logs for all sensitive utilities; thus, DISA DECC-St. Louis could not review program use violations.
Control Activity: SS-2.2 Inappropriate or unusual activity is investigated and appropriate actions taken.		
<u>DISA</u> DISA DECC-Mechanicsburg implemented an audit log review spreadsheet as of January 3, 2005, which is used to identify activities that warrant follow-up. The audit log review spreadsheets for each domain are made available to senior management via shared network folders. The Security Division Branch Chief will periodically monitor these files to help ensure the logs are monitored and to review trends. DISA DECC-Mechanicsburg relies on the automated security reporting features of ACF2. ACF2 generates reports from raw System Management Facility (SMF) records based on type of activity (e.g., log-on ID modification, dataset access violation, etc.). Similarly, DISA DECC-St. Louis relies on the automated security reporting features of Top Secret. The OS/390 STIG requires the DECC to review the ACF2 and Top Secret global control options at least quarterly to determine whether any changes were authorized and necessary.	<ul style="list-style-type: none"> Inquired to determine whether all changes to security profiles by security managers were automatically logged and periodically reviewed by management independent of the security function. Inquired of security administrators and inspected logs to determine whether unusual activity was investigated. 	<ul style="list-style-type: none"> Log data of changes to ACF2 and Top Secret security profiles were not consistently maintained and archived on the mainframe across the six ASIMS (one Top Secret, five ACF2) domains. As a result: <ul style="list-style-type: none"> No ACF2 log review evidence existed, to include changes to ACF2 security profiles, or violation logs prior to January 3, 2005. No Top Secret log review evidence existed, to include changes to security profiles, or violation logs. Sufficient contact information did not exist to adequately follow-up on issues identified during review of the logs. The contacts listed on the logs were not the appropriate contacts.
Control Activity: SS-3.1 System software changes are authorized, tested, and approved before implementation.		
<u>DISA</u> DISA DECC-St. Louis uses change request templates for	<ul style="list-style-type: none"> Inquired of the DISA DECC-St. Louis TSB 	<ul style="list-style-type: none"> DISA did not develop system software

Control Description	Tests of Operating Effectiveness	Results of Tests of Operating Effectiveness
<p>system software changes. Configuration Control Board (CCB) Instructions to be Followed for Preparation of Configuration Change Proposal (CCP) requires the following details for changes: major project/goal, change description, scope of change, domains affected, back-out procedures, downtime, and special instructions.</p> <p>SSO Mechanicsburg is responsible for building, testing, and distributing implementation-ready Mainframe Executive Software Suites for all test and production LPARs. This includes all software changes, releases, maintenance, and upgrades. The DECC and SSO technical staff participate in testing of system software changes, coordinate the scheduling, customer interfaces and administrative changes, implement the revised software suites, and provide operational technical support.</p> <p>If the proposed change impacts DISA DECC-St. Louis customers, a formal synopsis of the change is sent to the customers affected for coordination purposes.</p> <p>The REMEDY help desk ticket system tracks any identified problems.</p> <p>Emergency system software changes follow the same process as any other system software change, only the process is expedited.</p> <p>SSO is responsible for the standardization and optimization of the executive software suites for all DECCs. The Executive Support Plan documents and delegates these responsibilities to the SSO. The support plan states that the SSO will provide three levels of support: Standard Operating Environment (SOE), Centrally Supported Systems (CSS), and Consolidated Maintenance Contract (CMC).</p> <p>DISA DECC-Mechanicsburg employs a change management process for all software changes/requests called the ESCCB. An individual making a request for a change to or for new</p>	<p>Chief regarding procedures for making changes to system software supporting STANFINS.</p> <ul style="list-style-type: none"> Inspected system software change logs to determine whether system software changes on the STANFINS-related mainframe domains were tracked. Selected a random sample of changes to STANFINS system software/DB changes to determine whether required documentation was present. Inspected the notification e-mails for STANFINS changes applied during the examination period to determine whether implementation dates for STANFINS were communicated to personnel implementing the changes in the TSB. Inquired of STANFINS system owners and System Administrators to determine whether procedures were developed and documented for identifying and recording and tracking STANFINS-related system software problems. 	<p>change management procedures detailing specific DECC roles, responsibilities, and procedures regarding identification of system software problems, testing of changes, impact analyses, approvals, implementation and verification, and documentation requirements.</p> <ul style="list-style-type: none"> No audit log was created for the use of sensitive system utilities on the ACF2 domains; thus, DISA DECC-St. Louis could not review program use violations. Top Secret was not consistently configured to generate audit logs for all sensitive utilities; thus, DISA DECC-St. Louis could not review program use violations. DISA SSO and DISA DECC-St. Louis lacked change documentation that included detailed information about the change, such as test results or impact analysis. No exceptions noted. DISA did not develop system software change management procedures detailing specific DECC roles, responsibilities, and procedures regarding identification of system software problems, testing of changes, impact analyses, approvals, implementation and verification, and

Control Description	Tests of Operating Effectiveness	Results of Tests of Operating Effectiveness
<p>software must submit a request via a Web-based form. The ESCCB board meets on a weekly basis to review the requests submitted over the past week. The policies and procedures of the board set forth the process for submission and approval of change requests.</p> <p>Applicable domains track system software changes.</p>	<ul style="list-style-type: none"> Inspected vendor support agreements to determine whether they were current and provided coverage for computer assets. Inquired of management to determine whether tested and approved STANFINS system software migrated to the production environment was performed by an independent library control group. Compared user listings for individuals with access to migrate changes into the production environment to determine whether it was commensurate with job responsibilities. Inquired of DISA DECC-St. Louis TSB Branch Chief and inspected documentation system-generated inventories to determine whether DISA DECC-St. Louis maintained an inventory of programs on STANFINS-related mainframe domains. 	<p>documentation requirements.</p> <ul style="list-style-type: none"> No exceptions noted. The TSB migrated tested and approved system software changes; however, there were no documented policies requiring migration of system software changes into production by an independent library control group. The same person could develop/identify the change request, test the proposed change, and implement the change. At the DECC-Mechanicsburg, two individuals listed as authorized users for the Software Factory no longer required access. No exceptions noted.
<p><u>DFAS</u></p> <p>The CDOIM/DOIM is responsible for locally identifying and tracking problems related to STANFINS. CDOIM/DOIM maintains a copy of a log of all system problems. The log itself is not STANFINS specific; however, problems related to STANFINS are on the list.</p>	<ul style="list-style-type: none"> Inquired of the TSO and CDOIM IT Specialists and inspected CDOIM Operations Management Plan to determine whether procedures existed for identifying and documenting STANFINS-related system software changes. 	<ul style="list-style-type: none"> No exceptions noted.
<p>Control Activity: SS-3.2 Installation of system software is documented and reviewed.</p>		
<p><u>DISA</u></p> <p>DISA DECC-St. Louis tests patches, upgrades, and new system</p>	<ul style="list-style-type: none"> Inspected system software change logs to 	<ul style="list-style-type: none"> No audit log was created for the use of

Control Description	Tests of Operating Effectiveness	Results of Tests of Operating Effectiveness
<p>software depending on the nature of the change or product.</p> <p>DISA DECC-St. Louis maintains a list of all software on their systems in the Integrated Assets Configuration Management System database.</p> <p>Any request for new system software or upgrades to existing system software must be coordinated through the SSO. The SSO packages all software for transmission to DISA DECC-St. Louis.</p>	<p>determine whether system software changes on the STANFINS-related mainframe domains were tracked.</p> <ul style="list-style-type: none"> Selected a random sample of changes to STANFINS system software/DB changes to determine whether required documentation was present. Inquired of DISA DECC-St. Louis TSB Branch Chief and inspected system-generated inventories to determine whether DISA DECC-St. Louis maintained an inventory of programs on STANFINS-related mainframe domains. 	<p>sensitive system utilities on the ACF2 domains; thus, DISA DECC-St. Louis could not review program use violations.</p> <ul style="list-style-type: none"> Top Secret was not consistently configured to generate audit logs for all sensitive utilities; thus, DISA DECC-St. Louis could not review program use violations. DISA SSO and DISA DECC-St. Louis lacked change documentation that included detailed information about the change, such as test results or impact analysis. No exceptions noted.

Service Continuity (SC) – Backup and Recovery

Controls provide reasonable assurance that computer systems are backed up on a periodic basis and that procedures are employed to maintain the integrity of media.

Control Description	Tests of Operating Effectiveness	Results of Tests of Operating Effectiveness
Control Activity: SC-2.1 Data and program backup procedures have been implemented.		
<p><u>DISA</u></p> <p>Individual jobs are created to run the routine backups based on the domains that STANFINS resides on. A weekly backup job for the ASIMS domain is executed between Sunday evening and Monday morning. During the same weekly backup cycles, operating system and system utility programs are also backed up. Application and operating system/system software utility programs are not backed up to the same piece of media or collocated during storage.</p> <p>Within 1 or more of 49 StorageTek tape management silos located at the DISA DECC-St. Louis, backups are recorded to data tapes, which are ejected and placed into fireproof storage in a locked tape library until they are rotated to the off-site storage location. Tape library procedures outline tape handling procedures and responsibilities.</p> <p>The tape management system provides for an index of backup tapes, backup statuses, rotation schedules, etc. When data is recorded to backup tapes erroneously due to program failure or tape media integrity issues, the tape management system automatically detects these errors and produces reports that identify tapes containing errors. Additionally, the integrity of tape media is tested during the annual Continuity of Operations Plan (COOP) exercise during which backup tapes are restored, as well as by the tape management system immediately after the creation of the backup.</p> <p>Backup tapes are rotated off-site for three weeks and then returned to the DISA DECC-St. Louis facility for reuse. The only time the tapes are deposited or removed are during the</p>	<ul style="list-style-type: none"> • Inquired of the Operations Manager regarding the backup process and inspected the backup procedures to determine whether a process was developed and documented. • Inquired of Chief of the Capacity Management Branch (CMB) and inspected checklists for backing up STANFINS application files and programs, and key GSS operating systems, configurations, and tape library procedures to determine whether a process was developed and documented to regularly back up data and programs. • During a tour of the computer center, observed equipment to note whether tape management silos were used for physical tape management during the backup process. • Observed a weekly COOP dump process to verify that secondary tapes were created and sent to the offsite storage facility. • Inspected individual pickup/delivery receipts from July 2004 to October 2004 to determine whether tapes were picked up for off-site storage and returned by the off-site storage vendor. 	<ul style="list-style-type: none"> • No exceptions noted. • No exceptions noted. • No exceptions noted. • No exceptions noted. • No exceptions noted.

Control Description	Tests of Operating Effectiveness	Results of Tests of Operating Effectiveness
<p>weekly delivery/pickup of the off-site storage vendor. These actions are logged through the required delivery/pickup receipts. During transit to and from the off-site storage location, tapes are stored in fireproof containers.</p> <p>The off-site processing facility is physically removed from the DISA DECC-St. Louis backup storage site; approximately 35 miles separate the DECC from the backup storage site.</p> <p>DISA has contracted with the off-site storage facility to provide for physically secure and environmentally sound storage of backup tapes, which are accessible for disaster/recovery 24 hours a day/ 365 days of the year.</p>	<ul style="list-style-type: none"> • Inspected the offsite inventory listing that accompanies the tapes to the offsite storage facility that contained creation and expiration dates of the tapes and specific storage/rotation requirements to determine whether an inventory was documented. • Inquired of the Chief of the CMB and inspected COOP test results to determine whether tapes were tested during the annual COOP exercise, as well as by the tape management system immediately after creation of the backup. • Inquired of Chief of the Security Division and Chief of the CMB and inspected the contract with the offsite storage provider to determine whether the offsite storage was geographically removed from the DECC. • Inspected the contract for storage services to determine whether a current agreement existed between the offsite storage provider and the DISA DECC-St. Louis. 	<ul style="list-style-type: none"> • No exceptions noted. • No exceptions noted. • No exceptions noted. • No exceptions noted.

Service Continuity (SC) – Physical Computer Asset Protection

Administrative and operational controls should be established to provide reasonable assurance of the protection of physical computing assets.

Control Description	Tests of Operating Effectiveness	Results of Tests of Operating Effectiveness
Control Activity: SC-2.2 Adequate environmental controls have been implemented.		
<p><u>DISA</u></p> <p>DISA leases the DECC facility from the GSA. In addition to its capacity as leaseholder, GSA is responsible for maintaining environmental control devices (i.e., fire suppression systems; heating, ventilation, and air conditioning (HVAC); generators, etc.) and periodically inspects them to observe that they are working properly. Because GSA is responsible for the maintenance of environmental controls, the appropriate GSA personnel undergo initial and periodic training in the operation and support of the environmental controls.</p> <p>Fire detection and suppression systems have been installed at the DECC. Within the DECC's data center there are three levels of smoke detection. There are smoke detectors placed below the raised floor, mid-way up the data center walls, and on the ceiling of the data center. Each smoke detector can independently detect the presence of smoke. A dry pipe sprinkler system is activated upon triggering of the alarm system. There are also a total of 19 fire extinguishers throughout the data center. Additionally, smoke detectors are installed in the administrative/office areas of the DECC. GSA performs an annual test of each smoke detector in the DISA DECC-St. Louis facility.</p> <p>There are four chilling units that support the HVAC system in place for the data center. Because only one unit is required to cool the entire data center, the HVAC system is redundantly architected to provide uninterrupted cooling for the data center should units simultaneously fail.</p> <p>Humidity controls are placed throughout the data center, and personnel monitor them. Automated monitors poll gauges</p>	<ul style="list-style-type: none"> • Inspected the contract between GSA and DISA to determine responsibilities for maintenance of environmental protection mechanisms. • Toured the DECC facility and observed physical environment protection mechanisms to note whether the following controls were placed into operation: <ul style="list-style-type: none"> • Smoke detectors; • Raised flooring; • Dry pipe sprinkler systems; • Fire extinguishers; • HVAC systems; • Humidity monitors and alarms; • UPS; • Diesel generators; • Emergency lighting; • Exit signs; and • Emergency power cut-off buttons. • Inspected a contract regarding testing and equipment maintenance for the following environmental protection mechanisms: <ul style="list-style-type: none"> • Fire suppression devices; • Diesel generators and engine controls; • Underground storage tank; • Switchgear system; 	<ul style="list-style-type: none"> • No exceptions noted. • No exceptions noted. • No exceptions noted.

Control Description	Tests of Operating Effectiveness	Results of Tests of Operating Effectiveness
<p>hourly and compare humidity levels to predefined “acceptable” thresholds. Humidity gauges are linked to an alarm in the SMC. GSA personnel monitor and adjust the humidity controls and the other environmental controls located in the SMC.</p> <p>DISA DECC-St. Louis’s power supply is configured to switch automatically between the two commercial power feeds should one line fail. An Uninterruptible Power Supply (UPS) conditions electricity flowing on the feeds to eliminate spikes and sags. In the event that both commercial power feeds fail, the system is configured to automatically switch to battery power provided by the UPS while one or more of the four backup diesel generators are started. The transition usually takes less than one minute. Once the diesel generators are running, the power feed is automatically switched to the diesel generator(s).</p> <p>GSA activates the generators twice a year for testing purposes and services generators with regular and as-necessary maintenance.</p> <p>Emergency lighting during emergency exits and evacuation routes do not provide an exact route; however, they are adequate for providing lighting to escape the building. Exit signs are displayed and illuminated at all times for easy identification in an emergency.</p> <p>There is a red emergency cut-off button near the two main entrances to the DECC’s data center. The button is labeled and protected by a clear plastic cover to prevent accidental shut-off.</p> <p>DISA maintains service contracts with IT equipment vendors that provide for two-hour response times in service level agreements (SLAs).</p>	<ul style="list-style-type: none"> • Day tank and fuel storage/handling system; • Ancillary and accessories equipment systems; • Lubrication system; • HVAC; • Ventilation and exhaust system; • Starting batteries and charging system; and, • Safety Shutdown & Alarm system. <ul style="list-style-type: none"> • Inquired of the Chief of the TSB and inspected recovery plan documents to determine whether SLAs were arranged with IT equipment vendors to provide for two-hour response times. 	<ul style="list-style-type: none"> • No exceptions noted.

Authorization (AN)

Controls provide reasonable assurance that only authorized transactions are entered into and processed by the system.

Control Description	Tests of Operating Effectiveness	Results of Tests of Operating Effectiveness
Control Activity: AN-1.1 Source documents are controlled and require authorizing signatures.		
<p><u>DFAS</u> Based on their origination point, transactions require authorization from the appropriate Installation Representative (i.e., Budget Officer, Program Director) or DFAS.</p> <p><i>Installation-Originating Transactions</i> Installations send key source documents such as Transmittal Letters (TLs), FADs, APC, Add/Change requests, or other requests to generate a transaction to DFAS via mail, e-mail, and fax. Each of the significant classes of transactions can originate from the installation including Funding, Obligations, Disbursements, Transactions by Others (TBO), Collections, Reimbursables, and APC Masterfile Maintenance. The authorization process is the same for each.</p> <p>The DFAS Accounting Technician performs a visual review to determine whether an appropriate individual has authorized the key source document. DFAS maintains an authorized point of contact listing for each of their customers and/or signature verification cards to aid Accounting Technicians in the performance of their reviews. Should DFAS obtain source documents from individuals not identified as authorized points of contact, DFAS will not process the request and contact the appropriate authorized point of contact for resolution.</p> <p><i>DFAS-Originating Transactions</i> Transactions originating within DFAS include error corrections, journal vouchers, and control cards.</p> <p><u>Error Corrections</u> The AVK018, Daily Preliminary Balance, is the primary report used to identify data entry errors. Control Group or</p>	<p><i>AVK018 Report:</i></p> <ul style="list-style-type: none"> Observed the entry of invalid alphanumeric characters, incomplete fields, incorrect APCs, and invalid total cards. Inspected documentation to verify the error was included in the AVK018 report with appropriate coding. Verified that report was being reviewed to correct exceptions. <p><i>Control Cards</i></p> <ul style="list-style-type: none"> Inquired of management to determine whether accounting technicians and supervisors validated the data input into the STANFINS daily cycle. Inspected evidence of control was documented. 	<ul style="list-style-type: none"> Of 9 DFAS Field Sites tested, DFAS-Indianapolis, DFAS-Seaside, DFAS-Japan, DFAS-Lawton, DFAS-Rome, DFAS-Columbus, DFAS-Pacific, and DFAS-San Antonio, no standard procedures were maintained or enforced to ensure that errors were properly reconciled, authorized, corrected, and documented. DFAS-Denver, DFAS-Pacific, DFAS-Rome, DFAS-Seaside, DFAS-Indianapolis, DFAS-Columbus, DFAS-Japan, DFAS-San Antonio and DFAS-Lawton did not maintain documented evidence/signatures or note who performed the corrections and whether the correction was appropriate.. DFAS-Denver, DFAS-San Antonio, DFAS-Seaside, DFAS-Rome, and DFAS-Pacific of the 6 sites tested, did not maintain documented standard operating procedures related to the review of the control cards. DFAS-Orlando, DFAS-Indianapolis, DFAS-Denver, DFAS-San Antonio and DFAS-Columbus did not perform an independent or supervisory review of the control cards.

Control Description	Tests of Operating Effectiveness	Results of Tests of Operating Effectiveness
<p>Accounting Technicians use OLRV to retrieve the AVK018 report. The Accounting Technician reviews the report, performs research, and hand marks the types of corrective action needed on the report (generally via an update entered by the Accounting Technician through the TAPS). The error correction is applied upon the original block ticket number assigned in STANFINS unless the transaction is released (deleted) and re-input. DFAS Accounting Technicians and Accountants have been identified as trusted agents on behalf of the DFAS and the installation, and as such, do not obtain additional authorization to correct transaction errors.</p> <p><u>Control Cards</u> Control cards, or the files that are used to set various parameters that control that day's STANFINS batch processing cycle are either manually input or set within STANFINS via a macro program (a preprogrammed series of computer commands). Parameters set within control cards are visually reviewed to determine whether they were input properly. Some DFAS sites make a notation on printouts as evidence of their review, while others perform a visual review with no notations. Some DFAS sites maintain the reports while others do not. The Systems Office generates the cycles each day at a scheduled time or upon request of the Accountant/Accounting Technician.</p>		
<p>Control Activity: AN-2.1 Data entry terminals are secured and restricted to authorized users.</p>		
<p><u>DISA</u> The DISA Computing Services Security Handbook details granting access to system resources.</p> <p>Users at the DISA DECC-St. Louis have access to STANFINS application production files and data as necessary to support system operation and respond to customer requests. DECC users also have access to the mainframe GSS where the application resides. The DECC is responsible for creating and maintaining DECC user accounts, as well as DFAS ISSO and TASO accounts at customer sites. The local ISSO/TASO is responsible for creating and maintaining user accounts at</p>	<ul style="list-style-type: none"> • Inspected policies and procedures for granting and monitoring access to STANFINS IT resources. • Inquired of DISA DECC-St. Louis Security Division Branch Chief to determine the process for granting access to STANFINS and the GSS. • Inspected access control procedures to determine whether the process for granting, 	<ul style="list-style-type: none"> • No exceptions noted. • No exceptions noted. • No exceptions noted.

Control Description	Tests of Operating Effectiveness	Results of Tests of Operating Effectiveness
<p>customer sites.</p> <p>Users at the DECC (the majority of which are system software maintenance personnel) requiring access to the mainframe environment complete a form DD (Department of Defense) 2875 System Authorization Access Request, used for initial access requests, as well as for changes to an account. An authorized supervisor must sign this form, indicating approval of the access. Users must possess a security clearance commensurate with the classification level of the system in order to obtain access. Passwords are communicated to users via secure means, either in person or via e-mail, using separate e-mails to transmit user ID and password.</p> <p>The RAS server connections provide direct dial-in access to the network. DECC users requesting remote access must submit an approved access request form (Form DD 2875). Remote access is granted to users with a valid need, which must be approved by a supervisor, to access the network remotely. Typically, users are granted remote access in order to respond quickly to emergency situations and resolve problems when not at the DECC facility. After receiving an approved remote access request, the Security Division staff adds the user to the RAS server.</p> <p>The STANFINS application and the system software it resides on are protected through the mainframe access control applications CA-ACF2 and CA-Top Secret.</p> <p>Discretionary access controls are enforced through ACF2 and Top Secret mainframe security software. Also, access to shared and networked file systems outside the mainframe environment is controlled through discretionary access controls enforced through network access privileges.</p> <p>The UML Standardization memo establishes user ID rules for DECC users. DECC user IDs are configured to identify the user's department, as well as employment status. Additionally, the OS/390 STIG requires a unique ACF2 or Top Secret user</p>	<p>monitoring, and removing access to STANFINS followed Federal (NIST SP 800-26 – Logical Access) and DoD guidance (DoD Instruction 8500.2 – Remote Access, Access Procedures, Access Control Policies, Contractor and Foreign Nationals Access, Comprehensive Account Management, Least Privilege Procedures, Classified Data Protection).</p> <ul style="list-style-type: none"> Inspected access forms for a random sample of users of STANFINS (at the application and network level) to determine whether management authorized access). Inquired of DISA DECC-St. Louis Security Division Branch Chief regarding policies and procedures for recertifying users access in STANFINS. Obtained and inspected the ACL for STANFINS to determine whether terminated employees had access. 	<ul style="list-style-type: none"> At DISA DECC-St. Louis, we selected 42 users out of 1441 and requested their user access request form packets. Out of the sample of 42 packets: <ul style="list-style-type: none"> One user did not have a completed access request form; Three individuals had at least one access request form without a Security representative's signature certifying that the individual's background checks/security clearances were appropriate; Six individuals had at least one access request form where the user acknowledgement portion was not signed. DISA DECC-St. Louis did not have a process for recertifying user access to STANFINS. Two separated DISA DECC-St. Louis employees retained access to one or more of the domains where STANFINS resides.

Control Description	Tests of Operating Effectiveness	Results of Tests of Operating Effectiveness
<p>ID for every user.</p> <p>Passwords are not displayed as a user logs in to the mainframe. After three invalid log-on attempts, ACF2 automatically terminates the session. For the Top Secret domains, Top Secret suspends the user's account after two invalid log-on attempts.</p> <p>Before authentication, a warning banner is displayed that informs the user that the system is for authorized use only and that activity will be monitored. The terminal session automatically logs the user off after 15 minutes of inactivity and a screen-lock appears after 15 minutes, which requires the user to re-authenticate in order to re-gain access.</p> <p>Inactive accounts are suspended after 35 days of inactivity and deleted after 90 days of inactivity.</p>	<ul style="list-style-type: none"> Inspected ACL to determine whether duplicate accounts existed. Inspected an ACL of remote users and inquired of an ISSO to determine whether the access was limited, documented, and approved. Inquired of Security Division Branch Chief and Security Administrators and inspected ACF2 and Top Secret security settings to determine whether the security products were configured in accordance with OS/390 STIG guidance to enforce discretionary access controls. 	<ul style="list-style-type: none"> No duplicate accounts were identified. (No exception noted) However, three accounts on the Far East domain had no user name associated with the ACID. (Exception noted) Remote access to the DISA DECC-St. Louis mainframe via telnet was not restricted and not secured via encryption. Minimum password length on each of the five ACF2 ASIMS domains and the one Top Secret ASIMS domain was configured to six characters, while the OS/390 STIG requires passwords have a minimum of eight characters. Users on the Top Secret ASIMS domain were not required by the system to use a national character (e.g., \$, @, #) when creating new passwords, as required by the OS/390 STIG. Users on the ACF2 ASIMS domains were restricted from using their previous four passwords; users should be restricted from using their previous ten passwords as required by the OS/390 STIG. The Huntsville ASIMS domain had the JOBCK setting set to NOJOBCK. This setting did not require ACF2 to verify whether a user submitting a batch job has been granted the authority to submit batch

Control Description	Tests of Operating Effectiveness	Results of Tests of Operating Effectiveness
	<ul style="list-style-type: none"> Inspected the UML Standardization memo to determine whether naming conventions were established for DECC users. Inquired of Security Division Branch Chief and system administrators to determine security procedures for logging on and using the network. Inspected GSS (mainframe) policies and procedures to determine whether security procedures were documented. Inquired of Security Division Branch Chief and inspected procedures to determine whether inactive mainframe user accounts were monitored and removed when not 	<p>jobs.</p> <ul style="list-style-type: none"> An individual user was assigned to the Master Central Security Administrator (MSCA) account on the Top Secret ASIMS Far East domain. The MSCA designation allows full system access and is not required for individual users. 26 DECC ACF2 accounts on the ASIMS domains had passwords that did not expire (MAXDAYS not specified). 147 DECC Top Secret accounts on the Far East ASIMS domains had passwords that did not expire (Password Interval = 0). DECC users had “Write” or “Allocate” access to STANFINS production application datasets on two of five ACF2 ASIMS domains and the Top Secret ASIMS Far East domain. No exceptions noted. No exceptions noted. 451 ACF2 and 108 Top Secret DECC user accounts across the six STANFINS-related ASIMS domains were inactive for over 180

Control Description	Tests of Operating Effectiveness	Results of Tests of Operating Effectiveness
	<p>needed. Inspected the Top Secret and ACF2 STANFINS-related domain ACLs to determine whether inactive DECC user IDs were present in the domains.</p> <ul style="list-style-type: none"> Observed an individual user sign on to the mainframe to determine whether the opening screen provided a warning banner that stated that the system was for authorized use only and that activity was monitored. Observed a PC terminal to determine whether automatic log-off occurred after a preset number of minutes of inactivity. 	<p>days or had never been used.</p> <ul style="list-style-type: none"> No exceptions noted. No exceptions noted.
<p>DFAS</p> <p>The Procedures for ASIMS Access Controls details policies on security access responsibilities and the process to grant user access to STANFINS. DFAS uses user access forms to document the establishment, modification, deletion, or suspension of access to STANFINS IT resources, to include the STANFINS application, as well as the ELAN, used by DFAS administrative and field sites gain access to STANFINS.</p> <p>To set up ELAN access, the ELAN administrator, prior to establishing a network user ID and password, must approve the ELAN user access form via signature. For some sites, a separate security group approves the form via signature.</p> <p>Users must have a TAPS account in order to access the STANFINS application. The local TASO/ISSO is responsible for security administration, including the assignment of TAPS accounts. The ISSO creates user accounts for TAPS/STANFINS through a tool called VASS. For the majority of DFAS field sites, Microsoft Excel spreadsheet, Access database, or other manual means of tracking are used to identify STANFINS/TAPS users, TAPS mode profiles, and assigned TAPS modes. At DFAS-Orlando and DFAS-Japan,</p>	<ul style="list-style-type: none"> Inspected DFAS policies and procedures to determine whether guidance was established to outline ELAN administrator security responsibilities. Inspected access control procedures to determine whether the process for granting, monitoring, and removing access to STANFINS and GSS followed Federal (NIST SP 800-26 – Logical Access) and DoD guidance (DoD Instruction 8500.2 – Remote Access, Access Procedures, Access Control Policies, Contractor and Foreign Nationals Access, Comprehensive Account Management, Least Privilege Procedures, Classified Data Protection). 	<ul style="list-style-type: none"> Of the ten DFAS sites, DFAS-Indianapolis (PMO and TSO), DFAS-Pacific, DFAS-Japan and DFAS-Rome stated that there was no DFAS service-wide policy or guidance document outlining local ELAN administrator security responsibilities versus those of centralized groups responsible for the administration/ monitoring of DFAS-wide network security. During testing, DFAS field sites were unable to generate STANFINS and TAPS user access lists directly from the security system. As a result, of the ten DFAS field sites, DFAS-Rome, DFAS-Denver, DFAS-San Antonio, DFAS-Lawton, DFAS-Columbus, DFAS-Indianapolis and DFAS-Pacific, DFAS-Seaside DFAS field sites could not: <ul style="list-style-type: none"> Identify all TAPS modes (access privileges) assigned to users;

Control Description	Tests of Operating Effectiveness	Results of Tests of Operating Effectiveness
<p>TASOs/ISSOs generate ACF2-native listings in order to identify and track who has access to TAPS and STANFINS.</p> <p>The DFAS ISSP provides guidance in conducting monthly recertifications of STANFINS and ELAN accounts. The ISSO is responsible for providing each supervisor with a STANFINS user listing of access levels, and it is the supervisor's responsibility for validating and authorizing user access.</p> <p>Remote network access via the DISP accounts is granted to users with a valid need, which must be approved by a supervisor.</p> <p>STANFINS application password and user ID rules are configured in the security system software maintained by DISA.</p> <p>DFAS ELAN procedures include requirements that guide ELAN administrators in the conduct of network security administration.</p> <p>During log-in to the ELAN, there is a banner warning users that they are about to log on to a government workstation and that their use will be monitored. This banner automatically appears every time a user accesses any DFAS workstation connected to ELAN.</p> <p>ELAN workstations are CAC-configured, which means that an individual must insert a valid CAC card into a reader slot that is connected to the workstation in order to log in to the network. When the individual leaves the workstation, he or she must remove the CAC card from the reader slot, which automatically locks the workstation and prevents anyone else from accessing the workstation and LAN.</p>	<ul style="list-style-type: none"> Inspected access forms for a random sample of users of STANFINS (at the application and network level) to determine whether management authorized access. 	<ul style="list-style-type: none"> Determine whether users had inappropriate access to TAPS modes, based on job responsibilities; and Determine whether manually derived and maintained access control lists accurately reflected the user population. <ul style="list-style-type: none"> Of the ten DFAS field sites, nine field sites (DFAS-Rome, DFAS-Denver, DFAS-Lawton, DFAS-San Antonio, DFAS-Columbus, DFAS-Seaside, DFAS-Indianapolis, DFAS-Pacific and DFAS-Japan) either used locally developed or had not documented procedures for granting, approving, monitoring, recertifying, and removing user access to STANFINS and the ELAN. Six of ten DFAS user sites did not have complete or existing authorizations for STANFINS users as follows: DFAS-Denver: <ul style="list-style-type: none"> 18 STANFINS user access forms did not have an ELAN Account Request Form on file. DFAS-Pacific: <ul style="list-style-type: none"> Justification for STANFINS user access was pre-populated on user access forms by the TASOs and may not support actual needs. The functional data owner's signature was missing from TAPS user request forms on two of the eight forms inspected. DFAS-Japan: <ul style="list-style-type: none"> Four out of 31 ELAN access request forms that users filled out in 1998 did

Control Description	Tests of Operating Effectiveness	Results of Tests of Operating Effectiveness
		<p>not have an approval (signature).</p> <ul style="list-style-type: none"> Two external ELAN users had not signed user agreements. Seven out of 53 DD 2875/DISA 41 forms did not contain a business reason for the access request. One out of 53 DD 2875/DISA 41 forms did not contain a business case that adequately explained the reasoning for the access request. One out of 26 DISP User Access Request forms could not be found. Two out of 26 user access forms were not signed by the TASO. One out of 26 user access forms did not contain a supervisor signature or a business case justification. <p>DFAS-Rome:</p> <ul style="list-style-type: none"> Three out of 30 user access forms did not have authorization documentation available. 11 of 29 users with DISP accounts did not have a DISP user access request form with the appropriate approvals and/or justification. Two of these users had STANFINS accounts. <p>DFAS-San Antonio:</p> <ul style="list-style-type: none"> 32 out of 41 LAN user access forms did not have an access request form on file. <p>DFAS-Seaside:</p> <ul style="list-style-type: none"> 68 of 72 access request forms did not include an adequate business reason/justification for the access requested. 46 of 72 access request forms had a pre-populated response that included the type of access the user needed, but did

Control Description	Tests of Operating Effectiveness	Results of Tests of Operating Effectiveness
	<ul style="list-style-type: none"> • Inquired of DFAS field site ISSOs/TASOs to determine whether DFAS periodically recertified user access levels. • Inquired of DFAS ISSOs/TASOs, as well as DFAS field site supervisors, and inspected user access listings to TAPS/STANFINS to determine whether user access was commensurate with job responsibilities. • Observed an individual user sign on to the 	<p>not justify the access.</p> <ul style="list-style-type: none"> • Three out of 31 internal LAN user access forms did not have the functional data owner's signature. • 14 of 31 internal LAN user access forms did not have the original user access request form used to create their account. • Four of 31 internal users' access request forms were not signed by the information security officer. • There was no evidence of LAN access request forms or DISP user access request forms being used prior to February 10, 2005. • DFAS field sites did not have the technical knowledge to generate STANFINS and TAPS user access lists directly from the security system. At eight out of ten DFAS field sites (DFAS-Rome, DFAS-Denver, DFAS-Lawton, DFAS-San Antonio, DFAS-Columbus, DFAS-Seaside, DFAS-Indianapolis and DFAS-Pacific), the ISSOs/TASOs could not determine whether manually derived and maintained access control lists accurately reflected the user population, and therefore could not accurately perform user recertifications. • At DFAS-Columbus, DFAS-Japan, DFAS-Lawton, DFAS-San Antonio, DFAS-Pacific, DFAS-Rome and DFAS-Seaside, users had access that was not required by their job responsibilities.

Control Description	Tests of Operating Effectiveness	Results of Tests of Operating Effectiveness
	<p>network to determine whether the opening screen provided a warning banner that stated the system was for authorized use only and that activity was monitored.</p>	<ul style="list-style-type: none"> • No exceptions noted.

Completeness (CP)

Controls provide reasonable assurance that all authorized transactions are entered into and completely processed by the computer.

Control Description	Tests of Operating Effectiveness	Results of Tests of Operating Effectiveness
Control Activity: CP-1.1 Record counts and control totals.		
<u>DFAS</u> STANFINS uses a batch control method, called “blocking,” to determine whether control totals equal the sum of the details. During the daily production processing cycle, STANFINS performs batch edits for both manually entered transactions and transactions received through automated file loads. <i>Manual Input</i> Transactions manually entered through TAPS are subject to edits applied to automated transactions submitted for processing during the batch processing cycle. <i>Automated File Load</i> Transaction files may also be loaded via FTP. Similar to the TAPS edits, batch edits within STANFINS include the block totals. If a block total is not included in the FTP file, STANFINS will generate a block and then require a user to “accept” the block total within TAPS. The newly generated block will be reported on the Daily Preliminary Balance Report (AVK018). Transaction blocks identified as exceptions by batch edits are suspended and reported on the Daily Preliminary Balance Report (AVK018). Accounting Technicians review the AVK018 and clear erred transactions from the suspense file by submitting a correcting transaction, called a correction card, via TAPS. Items remain in suspense (and on the AVK018) until corrected. Blocks that do pass STANFINS batch edits are reported at a summary level by block in the AVK018.	<ul style="list-style-type: none">Observed STANFINS batch processing to note whether a block total entered that didn’t match the detailed transactions caused a suspended transaction. Inspected documentation to verify that these suspended transactions were recorded in the AVK018 report..	<ul style="list-style-type: none">No exceptions noted.
Control Activity: CP-1.3 Computer matching of transaction data.		
<u>DFAS</u>		

Control Description	Tests of Operating Effectiveness	Results of Tests of Operating Effectiveness
<p>During the daily production processing cycle, STANFINS performs batch edits for both manually entered transactions and transactions received through automated file loads.</p> <p><i>Manual Input</i> Transactions manually entered through TAPS are subject to edits applied to automated transactions submitted for processing during the batch processing cycle.</p> <p><i>Automated File Load</i> Similar to the TAPS edits, batch edits within STANFINS include:</p> <ul style="list-style-type: none"> • Alphanumeric checks; • Checks to determine whether required fields are populated such as Obligation Data Code, APC, and Fiscal Year; • Master file validations including data element relationship edits such as APC and Fiscal Year; and • Reconciliation of control totals to detail transaction totals (see control objective AC-10 for further information). <p>Transaction blocks identified as exceptions by batch edits are suspended and reported on the Daily Preliminary Balance Report (AVK018). Accounting Technicians review the AVK018 and clear erred transactions from the suspense file by submitting a correcting transaction, called a correction card, via TAPS. Items remain in suspense (and on the AVK018) until corrected. Blocks that do pass STANFINS batch edits are reported at a summary level by block in the AVK018.</p> <p>Additionally, STANFINS generates other reports to identify accounting issues. The accounting issues include, but are not limited to, Negative Unliquidated Obligations (reported in the AVK087 report), Obligations (NULOs) without an Accrual (AVK087), Credit Receivables (AVK024), and Over-obligations (AVK030 and AVK051). Accounting Technicians review these reports and work with the Program Directors to take corrective action, when applicable.</p>	<p><i>AVK018 Report:</i></p> <ul style="list-style-type: none"> • Observed the entry of invalid alphanumeric characters, incomplete fields, incorrect APCs, and invalid total cards. Inspected documentation to determine whether errors were included in the AVK018 report with appropriate coding and the report was being reviewed to correct exceptions. <p><i>AVK087 Report:</i></p> <ul style="list-style-type: none"> • Inquired of Systems Office Support management to determine if STANFINS automatically identified any abnormal accounting issues, such as NULOs (disbursements exceeding obligations), disbursements without obligations, accruals without obligations, accruals exceeding obligations, and negative obligation amounts. Inspected the resulting exception report, AVK087, and determined whether exceptions were properly identified. <p><i>AVK024 Report:</i></p> <ul style="list-style-type: none"> • Inquired with DNO management to determine how STANFINS determines if credit receivables were assigned to customers and if over earnings (exceeding the ceiling amount set for on the Military Interdepartmental Purchase Request (MIPR)) were assigned to customers. 	<ul style="list-style-type: none"> • Of 9 DFAS Field Sites tested, DFAS-Indianapolis, DFAS-Seaside, DFAS-Japan, DFAS-Lawton, DFAS-Rome, DFAS-Columbus, DFAS-Pacific, and DFAS-San Antonio, no standard procedures were maintained or enforced to ensure that errors were properly reconciled, authorized, corrected, and documented. • DFAS-Denver, DFAS-Pacific, DFAS-Rome, DFAS-Seaside, DFAS-Indianapolis, DFAS-Columbus. DFAS-Japan, DFAS-San Antonio and DFAS-Lawton did not maintain documented evidence/signatures or note who performed the corrections and whether the correction was appropriate.. • The design of the control was ineffective in that the AVK-087 report was not cumulative. Abnormal accounting situations were reported only once; therefore, after the following day, the report did not identify that the abnormal accounting situation existed. No test of operating effectiveness was performed, since the report could not be sampled. • No exceptions noted.

Control Description	Tests of Operating Effectiveness	Results of Tests of Operating Effectiveness
	<ul style="list-style-type: none"> Observed the processing of a credit receivable and an over earnings within STANFINS to determine whether the AVK024 identified the transaction. <p><i>AVK030 and AVK051 Report:</i></p> <ul style="list-style-type: none"> Observed the processing of a transaction that caused an over obligation. Inspected the appropriate AVK report to determine whether the report correctly identified the accounting issue. 	<ul style="list-style-type: none"> DFAS-San Antonio, DFAS-Denver and DFAS-Rome of the three DFAS field sites tested did not have documented procedures for identifying and resolving credit unfilled orders or credit receivables. The 2 DFAS field sites who use the STANFINS AVK024, DFAS-Rome and DFAS-Denver, did not maintain evidence that documented the authorization and correction of each corrected credit receivables or credit unfilled orders transaction. . No exceptions noted.
Control Activity: CP-1.4 Checking reports for transaction data.		
<p><u>DFAS</u></p> <p>Accounting Technicians review numerous reports to verify transactions and master file additions/changes processed successfully. Key reports identified include the AVK018 and the AVK003. Blocks that pass STANFINS batch edits are reported at a summary level by block in the AVK018. The Accounting Technicians review the block totals on the AVK018 to ensure transactions processed accurately. The AVK003 (Master Update Listing) is reviewed to identify additions, changes, and deletions to the master file.</p>	<p><i>AVK003 Report:</i></p> <ul style="list-style-type: none"> Observed the entry of a new APC and inspected the AVK003 to determine whether the APC was included on the report. <p><i>AVK018 Report:</i></p> <ul style="list-style-type: none"> Observed the entry of invalid alphanumeric characters, incomplete fields, incorrect APCs, and invalid total cards. Inspected documentation to determine whether the error was included in the AVK018 report with appropriate coding and the report was being reviewed to correct exceptions 	<ul style="list-style-type: none"> No exceptions noted. Of 9 DFAS Field Sites tested, DFAS-Indianapolis, DFAS-Seaside, DFAS-Japan, DFAS-Lawton, DFAS-Rome, DFAS-Columbus, DFAS-Pacific, and DFAS-San Antonio, no standard procedures were maintained or enforced to ensure that errors were properly reconciled, authorized, corrected, and documented.

Control Description	Tests of Operating Effectiveness	Results of Tests of Operating Effectiveness
		<ul style="list-style-type: none"> DFAS-Denver, DFAS-Pacific, DFAS-Rome, DFAS-Seaside, DFAS-Indianapolis, DFAS-Columbus, DFAS-Japan, DFAS-San Antonio and DFAS-Lawton did not maintain documented evidence/signatures or note who performed the corrections and whether the correction was appropriate..
Control Activity: CP-2.1 Reconciliations show the completeness of data processed at points in the processing cycle.		
<p><u>DFAS</u></p> <p>DFAS uses a manual method of batching, called “blocking,” to help ensure transactions are entered accurately. This manual method involves block tickets and block control logs (BCL). A block ticket is a DFAS-generated input document. The BCL is a manually maintained log that tracks all the blocks. Various DFAS field site divisions/branches and individual users within a branch employ different procedures with respect to the block tickets and BCL. In general, the control department or receiver receives the transmittal letters and other source documentation via phone, fax, or e-mail. The receiver then creates a block ticket and assigns a block number and records it on the BCL. The Accounting Technician then inputs the transaction into TAPS. The block ticket itself has a space for the verification along with a date. Initialing and dating this area indicates the input technician has visually compared the amount on the block ticket to the block total on the screen to help ensure accuracy.</p> <p>Additionally, some DFAS field site block tickets have a section to track when the block cleared the DPBL (Daily Preliminary Balance Report, also known as the AVK018 report). By initialing and dating the section, the user successfully traced the transaction from the block ticket to the AVK018 report, thus indicating that the transaction processed successfully.</p>	<ul style="list-style-type: none"> Inspected BCLs to determine whether they were reconciled to STANFINS batch control data. 	<ul style="list-style-type: none"> Of 5 DFAS field sites tested, DFAS-San Antonio and DFAS-Indianapolis did not have documented standard procedures to address reconciliation of BCLs. None of the DFAS field sites tested performed/maintained documentation of reconciliations of summary dollar amounts and/or block totals on the block ticket to summary data within STANFINS.

Accuracy (AY)

Controls provide reasonable assurance that transactions processed by the system maintain validity and accuracy throughout processing.

Control Description	Tests of Operating Effectiveness	Results of Tests of Operating Effectiveness
Control Activity: AY-1.3 Key verification increases the accuracy of significant data fields.		
<p>DFAS</p> <p>DFAS uses a manual method of batching, called “blocking,” to help ensure transactions are entered accurately. This manual method involves block tickets and BCL. A block ticket is a DFAS-generated input document. The BCL is a manually maintained log that tracks all the blocks. Various DFAS field site divisions/branches and individual users within a branch employ different procedures with respect to the block tickets and BCL. In general, the control department or receiver receives the transmittal letters and other source documentation via phone, fax, mail, electronic file, or e-mail. The receiver then creates a block ticket and assigns a block number and records it on the BCL. The Accounting Technician then inputs the transaction into TAPS. The block ticket itself has a space for “input by” along with a date. Initialing and dating this area indicates the input technician has visually compared the amount on the block ticket to the block total on the screen to help ensure accuracy.</p> <p>Depending on the user or division, there are various standards followed and levels of detail maintained on the BCL and block ticket. For example, some divisions use a Microsoft Access database to track blocks while others use a manually maintained BCL. Some divisions/users keep evidence of their review of the block summary indicated in the screen and others do not. Some divisions/users have different standards or definitions for the purpose of each of the fields on the block ticket and BCL. In some instances, the “input by” space on the block ticket indicates the input technician has visually compared the amount on the block ticket to the block total on the screen. In other instances, the “input by” space on the block ticket only indicates the input technician entered the transaction; not that the block total matched what had been</p>	<ul style="list-style-type: none"> Inspected BCLs to determine whether they contain the appropriate data and were reconciled to STANFINS batch control data. <p><i>AVK087 Report:</i></p> <ul style="list-style-type: none"> Inquired of Systems Office Support management to determine whether STANFINS automatically identifies any abnormal accounting issues, such as NULOs (disbursements exceeding obligations), disbursements without obligations, accruals without obligations, accruals exceeding obligations, and negative obligation amounts. Inspected the resulting exception report, AVK087, to determine whether exceptions were properly identified. <p><i>AVK024 Report:</i></p> <ul style="list-style-type: none"> Inquired with DNO management to determine how STANFINS determined if credit receivables were assigned to customers and if over earnings (exceeding 	<ul style="list-style-type: none"> Of 5 DFAS field sites tested, DFAS-San Antonio and DFAS-Indianapolis did not have documented standard procedures to address reconciliation of BCLs. None of the DFAS field sites tested performed/maintained documentation of reconciliations of summary dollar amounts and/or block totals on the block ticket to summary data within STANFINS. The design of the control for the <i>AVK087 Report</i> was ineffective in that the report was not cumulative. Abnormal accounting situations are reported only once; therefore, after the following day, the report did not identify that the abnormal accounting situation existed. No test of operating effectiveness was performed, since the report could not be sampled. No exceptions noted.

Control Description	Tests of Operating Effectiveness	Results of Tests of Operating Effectiveness
<p>expected.</p> <p>Additionally, some DFAS field site block tickets have a section to track when the block cleared the DPBL (Daily Preliminary Balance Report, also known as the AVK018 report). By initialing and dating the section, the user successfully traced the transaction from the block ticket to the AVK018 report, thus indicating that the transaction processed successfully.</p> <p>Also, TAPS and STANFINS have additional edit checks to help determine the accuracy of significant data.</p> <p><i>Manual Input</i> Transactions manually entered through TAPS are subject to edits applied to automated transactions submitted for processing during the batch processing cycle.</p> <p><i>Automated File Load</i> During the daily production processing cycle, STANFINS performs batch edits for manually entered transactions and transactions received through automated file loads. Similar to the TAPS edits, batch edits in STANFINS include:</p> <ul style="list-style-type: none"> • Alphanumeric checks; • Checks to determine whether required fields are populated such as Obligation Data Code, APC, and Fiscal Year; • Master file validations including data element relationship edits such as APC and Fiscal Year; and • Reconciliation of control totals to detail transaction totals (see control objective AC-10 for further information). <p>Transaction blocks identified as exceptions by batch edits are suspended and reported on the Daily Preliminary Balance Report (AVK018). Accounting Technicians review the AVK018 and clear erred transactions from the suspense file by submitting a correcting transaction, called a correction card, via TAPS. Items remain in suspense within STANFINS (and on the AVK018).</p>	<p>the ceiling amount set for on the Military Interdepartmental Purchase Request (MIPR)) were assigned to customers.</p> <ul style="list-style-type: none"> • Observed the processing of a credit receivable and an over earnings within STANFINS to determine whether the AVK024 identified the transaction. <p><i>AVK030 and AVK051 Report:</i></p> <ul style="list-style-type: none"> • Observed the processing of a transaction that caused an over obligation. Inspected the appropriate AVK report to determine whether the report correctly identified the accounting issue. 	<ul style="list-style-type: none"> • DFAS-San Antonio, DFAS-Denver and DFAS-Rome of the three DFAS field sites tested did not have documented procedures for identifying and resolving credit unfilled orders or credit receivables. • The 2 DFAS field sites who use the STANFINS AVK024, DFAS-Rome and DFAS-Denver, did not maintain evidence that documented the authorization and correction of each corrected credit receivables or credit unfilled orders transaction. • No exceptions noted.

Control Description	Tests of Operating Effectiveness	Results of Tests of Operating Effectiveness
Control Activity: AY-2.1 Programmed validation and edit checks identify erroneous data.		
<u>DFAS</u> <i>Manual Input</i> Transactions manually entered through TAPS are subject to edits applied to automated transactions submitted for processing during the batch processing cycle, as described in the section below. <i>Automated File Load</i> During the daily production processing cycle, STANFINS performs batch edits for manually entered transactions and transactions received through automated file loads. Similar to the TAPS edits, batch edits in STANFINS include: <ul style="list-style-type: none"> Alphanumeric checks; Checks to determine whether required fields are populated such as Obligation Data Code, APC, and Fiscal Year; Master file validations including data element relationship edits such as APC and Fiscal Year; and Reconciliation of control totals to detail transaction totals (see control objective AC-10 for further information). Transaction blocks identified as exceptions by batch edits are suspended and reported on the Daily Preliminary Balance Report (AVK018). Accounting Technicians review the AVK018 and clear erred transactions from the suspense file by submitting a correcting transaction, called a correction card, via TAPS. Items remain in suspense (and on the AVK018) until corrected. Blocks that do pass STANFINS batch edits are reported at a summary level by block in the AVK018. Additionally, STANFINS generates other reports to identify accounting issues. The accounting issues include, but are not limited to, Negative Unliquidated Obligations (AVK087), Obligations without an Accrual (AVK087), Credit Receivables (AVK024), and Over-obligations (AVK030 and AVK051).	<i>AVK018 Report:</i> <ul style="list-style-type: none"> Observed the entry of invalid alphanumeric characters, incomplete fields, incorrect APCs, and invalid total cards. Inspected documentation to determine whether the errors were included in the AVK018 report with appropriate coding and the report was being reviewed to correct exceptions. <i>AVK087 Report:</i> <ul style="list-style-type: none"> Inquired of Systems Office Support management to determine if STANFINS automatically identified any abnormal accounting issues, such as NULOs (disbursements exceeding obligations), disbursements without obligations, accruals without obligations, accruals exceeding obligations, and negative obligation amounts. Inspected the resulting exception report, AVK087, and to determine whether exceptions were properly identified. <i>AVK024 Report:</i> <ul style="list-style-type: none"> Inquired with DNO management to determine how STANFINS determines if credit receivables were assigned to customers and if over earnings (exceeding 	<ul style="list-style-type: none"> Of 9 DFAS Field Sites tested, DFAS-Indianapolis, DFAS-Seaside, DFAS-Japan, DFAS-Lawton, DFAS-Rome, DFAS-Columbus, DFAS-Pacific, and DFAS-San Antonio, no standard procedures were maintained or enforced to ensure that errors were properly reconciled, authorized, corrected, and documented. DFAS-Denver, DFAS-Pacific, DFAS-Rome, DFAS-Seaside, DFAS-Indianapolis, DFAS-Columbus. DFAS-Japan, DFAS-San Antonio and DFAS-Lawton did not maintain documented evidence/signatures or note who performed the corrections and whether the correction was appropriate.. The design of the control for the <i>AVK087 Report</i> was ineffective in that the report was not cumulative. Abnormal accounting situations are reported only once; therefore, after the following day, the report did not identify that the abnormal accounting situation existed. No test of operating effectiveness was performed, since the report could not be sampled. No exceptions noted.

Control Description	Tests of Operating Effectiveness	Results of Tests of Operating Effectiveness
<p>Accounting Technicians review these reports and work with the Program Directors to take corrective action, when applicable.</p>	<p>the ceiling amount set for on the Military Interdepartmental Purchase Request (MIPR)) were assigned to customers.</p> <ul style="list-style-type: none"> Observed the processing of a credit receivable and an over earnings in STANFINS to determine whether the AVK024 identified the transaction. <p><i>AVK030 and AVK051 Report:</i></p> <ul style="list-style-type: none"> Observed the processing of a transaction that caused an over obligation. Inspected the appropriate AVK report to determine whether the report correctly identified the accounting issue. 	<ul style="list-style-type: none"> DFAS-San Antonio, DFAS-Denver and DFAS-Rome of the three DFAS field sites tested did not have documented procedures for identifying and resolving credit unfilled orders or credit receivables. The 2 DFAS field sites who use the STANFINS AVK024, DFAS-Rome and DFAS-Denver, did not maintain evidence that documented the authorization and correction of each corrected credit receivables or credit unfilled orders transaction. No exceptions noted.

Control Description	Tests of Operating Effectiveness	Results of Tests of Operating Effectiveness
Control Activity: AY-2.3 Overriding or bypassing data validation and editing is restricted.		
<u>DFAS</u> <i>Manual Input</i> Should an Accounting Technician manually enter a transaction that TAPS edits identify as an exception, a warning message appears on the screen. During the TAPS edit process, users have the option to correct the transaction at this point. Additionally, users have the ability to bypass the warning message, thus allowing the transaction to continue processing. Transactions bypassed in TAPS and submitted for continued processing are subject to batch cycle edit checks. During the daily production processing cycle, STANFINS performs batch edits for manually entered transactions and transactions received through automated file loads. Similar to the TAPS edits, batch edits in STANFINS include: <ul style="list-style-type: none"> • Alphanumeric checks; • Checks to determine whether required fields are populated such as Obligation Data Code, APC, and Fiscal Year; • Master file validations including data element relationship edits such as APC and Fiscal Year; and • Reconciliation of control totals to detail transaction totals (see control objective AC-10 for further information). Transaction blocks identified as exceptions by batch edits are suspended and reported on the Daily Preliminary Balance Report (AVK018). Accounting Technicians review the AVK018 and clear erred transactions from the suspense file by submitting a correcting transaction, called a correction card, via TAPS. Items remain in suspense (and on the AVK018) until corrected. Blocks that do pass STANFINS batch edits are reported at a summary level by block in the AVK018.	<i>AVK018 Report:</i> <ul style="list-style-type: none"> • Observed the entry of invalid alphanumeric characters, incomplete fields, incorrect APCs, and invalid total cards. Inspected documentation to verify the inclusion in the AVK018 report with appropriate error coding. Verified that report was being reviewed to correct exceptions. <i>AVK087 Report:</i> <ul style="list-style-type: none"> • Inquired of Systems Office Support management to determine if STANFINS automatically identified any abnormal accounting issues, such as NULOs (disbursements exceeding obligations), disbursements without obligations, accruals without obligations, accruals exceeding obligations, and negative obligation amounts. Inspected the resulting exception report, AVK087 to determine whether exceptions were properly identified. <i>AVK024 Report:</i> <ul style="list-style-type: none"> • Inquiry with DNO management to determine how STANFINS identified that 	<ul style="list-style-type: none"> • Of 9 DFAS Field Sites tested, DFAS-Indianapolis, DFAS-Seaside, DFAS-Japan, DFAS-Lawton, DFAS-Rome, DFAS-Columbus, DFAS-Pacific, and DFAS-San Antonio, no standard procedures were maintained or enforced to ensure that errors were properly reconciled, authorized, corrected, and documented. • DFAS-Denver, DFAS-Pacific, DFAS-Rome, DFAS-Seaside, DFAS-Indianapolis, DFAS-Columbus. DFAS-Japan, DFAS-San Antonio and DFAS-Lawton did not maintain documented evidence/signatures or note who performed the corrections and whether the correction was appropriate.. • The design of the control was ineffective in that the <i>AVK087 Report</i> was not cumulative. Abnormal accounting situations were reported only once; therefore, after the following day, the report did not identify that the abnormal accounting situation existed. No test of operating effectiveness was performed, since the report could not be sampled. • No exceptions noted.

Control Description	Tests of Operating Effectiveness	Results of Tests of Operating Effectiveness
	<p>credit receivables were assigned to customers and if over earnings (exceeding the ceiling amount set for on the MIPR) were assigned to customers.</p> <ul style="list-style-type: none"> Observed the processing of a credit receivable and an over earnings in STANFINS to determine whether the AVK024 identified the transaction. <p><i>AVK030 and AVK051 Report:</i></p> <ul style="list-style-type: none"> Observed the processing of a transaction that caused an over obligation. Inspected the appropriate AVK report to determine whether the report correctly identified the accounting issue. 	<ul style="list-style-type: none"> DFAS-San Antonio, DFAS-Denver and DFAS-Rome of the three DFAS field sites tested did not have documented procedures for identifying and resolving credit unfilled orders or credit receivables. The 2 DFAS field sites who use the STANFINS AVK024, DFAS-Rome and DFAS-Denver, did not maintain evidence that documented the authorization and correction of each corrected credit receivables or credit unfilled orders transaction. No exceptions noted.
<p>Control Activity: AY-3.1 Rejected transactions are controlled with an automated error suspense file.</p>		
<p><u>DFAS</u> STANFINS maintains a suspense file, EXGAVK. The program that generates the suspended transaction report, AVK018, is called PBKAVK. A control group is responsible for controlling and monitoring the rejected transactions. Suspended blocks remain in suspense and on the report until corrected or released (deleted).</p> <p>Additionally, the Accounting Technician responsible for the AVK018 corrections researches the error and makes the corrections via TAPS. In most instances, the AVK018 and related backup documentation is kept for one year.</p>	<p><i>AVK018 Report:</i></p> <ul style="list-style-type: none"> Observed the entry of invalid alphanumeric characters, incomplete fields, incorrect APCs, and invalid total cards. Inspected documentation to determine whether errors were included the AVK018 report with appropriate coding and the report was being reviewed to correct exceptions. 	<ul style="list-style-type: none"> Of 9 DFAS Field Sites tested, DFAS-Indianapolis, DFAS-Seaside, DFAS-Japan, DFAS-Lawton, DFAS-Rome, DFAS-Columbus, DFAS-Pacific, and DFAS-San Antonio, no standard procedures were maintained or enforced to ensure that errors were properly reconciled, authorized, corrected, and documented.

Control Description	Tests of Operating Effectiveness	Results of Tests of Operating Effectiveness
		<ul style="list-style-type: none"> DFAS-Denver, DFAS-Pacific, DFAS-Rome, DFAS-Seaside, DFAS-Indianapolis, DFAS-Columbus. DFAS-Japan, DFAS-San Antonio and DFAS-Lawton did not maintain documented evidence/signatures or note who performed the corrections and whether the correction was appropriate..
Control Activity: AY-3.2 Erroneous data are reported back to the user department for investigation and correction.		
<u>DFAS</u> The Accounting Technician responsible for the AVK018 corrections researches the error and makes the corrections via TAPS. In most instances, the AVK018 and related backup documentation is kept for one year.	<i>AVK018 Report:</i> <ul style="list-style-type: none"> Observed the entry of invalid alphanumeric characters, incomplete fields, incorrect APCs, and invalid total cards. Inspected documentation to determine whether errors were included the AVK018 report with appropriate coding and the report was being reviewed to correct exceptions. 	<ul style="list-style-type: none"> Of 9 DFAS Field Sites tested, DFAS-Indianapolis, DFAS-Seaside, DFAS-Japan, DFAS-Lawton, DFAS-Rome, DFAS-Columbus, DFAS-Pacific, and DFAS-San Antonio, no standard procedures were maintained or enforced to ensure that errors were properly reconciled, authorized, corrected, and documented. DFAS-Denver, DFAS-Pacific, DFAS-Rome, DFAS-Seaside, DFAS-Indianapolis, DFAS-Columbus. DFAS-Japan, DFAS-San Antonio and DFAS-Lawton did not maintain documented evidence/signatures or note who performed the corrections and whether the correction was appropriate..

Control Description	Tests of Operating Effectiveness	Results of Tests of Operating Effectiveness
Control Activity: AY-4.2 Reports showing the results of processing are reviewed by users.		
<p><u>DFAS</u></p> <p>Accounting Technicians review numerous reports to verify processing results. Key reports identified include: AVK003, AVK006, and AVK018. The AVK003 (Master Update Listing) is reviewed to identify additions, changes, and deletions to the master files. The AVK006 (Master Update Error Report) is reviewed to identify lines that did not process to the master files along with respective error codes. As documented in AY 3.1, the AVK018 (Daily Preliminary Balance) is reviewed to ensure transactions processed accurately.</p>	<p><i>AVK018 Report:</i></p> <ul style="list-style-type: none"> Observed the entry of invalid alphanumeric characters, incomplete fields, incorrect APCs, and invalid total cards. Inspected documentation to determine whether errors were included the AVK018 report with appropriate coding and the report was being reviewed to correct exceptions. Inquired of management to obtain an understanding of the procedures to review the AVK006 report, research the errors, make associated corrections, and document, where appropriate, resolution of the error and authorizations. 	<ul style="list-style-type: none"> Of 9 DFAS Field Sites tested, DFAS-Indianapolis, DFAS-Seaside, DFAS-Japan, DFAS-Lawton, DFAS-Rome, DFAS-Columbus, DFAS-Pacific, and DFAS-San Antonio, no standard procedures were maintained or enforced to ensure that errors were properly reconciled, authorized, corrected, and documented. DFAS-Denver, DFAS-Pacific, DFAS-Rome, DFAS-Seaside, DFAS-Indianapolis, DFAS-Columbus. DFAS-Japan, DFAS-San Antonio and DFAS-Lawton did not maintain documented evidence/signatures or note who performed the corrections and whether the correction was appropriate.. DFAS-Rome, DFAS-Japan, DFAS-Columbus, DFAS-Denver, DFAS-Orlando and DFAS-San Antonio maintained limited or no evidence regarding the review, input, and resolution of the errors. DFAS-Seaside, DFAS-Japan, DFAS-Columbus, DFAS-Denver, DFAS-Orlando, DFAS-San Antonio did not maintain a policy or standard operating procedure documenting the evidence requirements supporting the correction for errors within the AVK006 report.

Integrity (IN)

Controls provide reasonable assurance that production processing uses the current version of software and data, that transactions are secured from unauthorized modification, and that concurrent updates of files are not allowed.

Control Description	Tests of Operating Effectiveness	Results of Tests of Operating Effectiveness
Control Activity: Production scheduling is monitored for program failures due to corrupted or missing input files.		
<u>Common Controls</u> ⁴ Control-M records the data and time, user ID and disposition code, and job execution message regarding the completion of production jobs to audit trails. Color-coding facilitates the identification of erred production jobs. Audit trails are generated real-time during the execution of the production schedule and are available for review after-the-fact. Control-M produces a log that identifies that a schedule change has been made and the user ID of the individual who made the change. Control-M has the ability to filter data to identify deleted schedules and the user who performed the deletion.	<ul style="list-style-type: none"> Inquired of IT Supervisor and Specialist and inspected the settings page to determine the settings applied for recording of audit records in SysLog. Inspected a screen print of the Control-M History log to determine whether audit trails of production schedule/job completion was documented. 	<ul style="list-style-type: none"> At the DOIM located in Denver, personnel were unaware of automated logging features in Control-M, stating there was no automated audit logging process for STANFINS job scheduling and processing. At the DOIM located in Denver, the audit trails for production job scheduling were not documented.
<u>DISA</u> DISA DECC-St. Louis and DISA DECC-Mechanicsburg share responsibility for monitoring of production processing with DFAS. When an operator at DECC identifies an abnormal job termination ABEND, he/she creates a REMEDY system ticket and contacts an appropriate DFAS point of contact (POC) for resolution. Contact lists/escalation procedures document POCs to be called in the event of unresolved ABEND. DISA DECC maintains historical REMEDY tickets as a resource for identifying and resolving production-processing problems. Once DFAS is alerted of the issue, DFAS is responsible for identifying a method of resolution and ensuring the problem is resolved.	<ul style="list-style-type: none"> Inquired with TSB personnel to determine whether a process for identifying, documenting, and tracking production schedule deviations was developed. Inspected the listing of appropriate DFAS points of contact to determine if contact information was documented. For production issues since July 2004, inspected the corresponding REMEDY tickets to determine if they were tracked to 	<ul style="list-style-type: none"> No exceptions noted. No exceptions noted. No exceptions noted.

⁴ Common controls are those controls that a DoD organization other than DISA or DFAS implements, and are commonly applied across both DISA and DFAS.

Control Description	Tests of Operating Effectiveness	Results of Tests of Operating Effectiveness
<p><u>DFAS</u> DISA DECC-St. Louis and DISA DECC-Mechanicsburg share responsibility for monitoring of production processing with DFAS.</p> <p>Once DFAS is alerted of the issue, DFAS is responsible for identifying a method of resolution and ensuring the problem is resolved.</p> <p>Some DOIM sites have standard operating procedures to address production job ABENDS and escalation procedures. Processing is monitored real-time and any issues are immediately identified and addressed. When a job encounters an ABEND, the screen turns red and processing stops until it is corrected and restarted by an operator.</p> <p>Escalation procedures provide detailed instruction on handling ABENDS and identify points of contact.</p> <p>In some cases, Internal Trouble Reports are created when STANFINS processing ABENDS. When an Internal Trouble Report is created, an approval must accompany the change made to fix the processing issue.</p>	<p>completion.</p> <ul style="list-style-type: none"> Inquired with Computer/EDP Specialist to determine whether a process for identifying, documenting, and tracking production schedule deviations was developed. Inspected procedures to determine whether the process was documented and whether a point of contact list was available for reference when problem escalation was necessary. Inspected procedures used for production processing and documentation used to track deviations from the predefined production-processing schedule. For production issues since July 2004, inspected the corresponding REMEDY tickets to determine if they were tracked to completion 	<ul style="list-style-type: none"> At the DOIM site located in Denver, <ul style="list-style-type: none"> Denver DOIM Management did not develop and implement Control-M standards and procedures to aid personnel in the use of this application. The process for documenting the job schedule changes and any issues during processing was informal. As a result, no documentation existed for these processes. A description of STANFINS production jobs, description of ABEND codes, and escalation, recovery, and restart procedures was not documented. At the DOIM site located in Denver, <ul style="list-style-type: none"> Denver DOIM Management did not develop and implement Control-M standards and procedures to aid personnel in the use of this application. The process for documenting the job schedule changes and any issues during processing was informal. As a result, no documentation existed for these processes. A description of STANFINS production jobs, description of ABEND codes, and escalation, recovery and restart procedures was not documented. No exceptions noted.
<p>Control Activity: A program change/confirmation management process is in place that includes testing changes prior to their introduction to the production environment.</p>		

Control Description	Tests of Operating Effectiveness	Results of Tests of Operating Effectiveness
<p><u>DISA</u> DISA DECC-St. Louis uses change request templates for system software changes. The CCB Instructions to be Followed for Preparation of CCP requires the following details for changes: major project/goal, change description, scope of change, domains affected, back-out procedures, downtime, and special instructions.</p> <p>SSO Mechanicsburg is responsible for building, testing, and distributing implementation-ready Mainframe Executive Software Suites for all test and production LPARs. This includes all software changes, releases, maintenance, and upgrades. The DECC and SSO technical staffs participate in the testing; coordinate the scheduling, customer interfaces, and administrative changes; implement the revised software suites; and provide operational technical support.</p> <p>If the proposed change impacts DISA DECC-St. Louis customers, a formal synopsis of the change is sent to the customers affected for coordination purposes.</p> <p>The REMEDY help desk ticket system tracks any identified problems.</p> <p>Emergency system software changes follow the same process as any other system software change, only the process is expedited.</p> <p>SSO is responsible for the standardization and optimization of the executive software suites for all DECCs. The Executive Support Plan documents and delegates these responsibilities to the SSO. The support plan states that the SSO will provide three levels of support: Standard Operating Environment (SOE), Centrally Supported Systems (CSS), and Consolidated Maintenance Contract (CMC).</p> <p>DISA DECC-Mechanicsburg employs a change management process for all software changes/requests called the ESCCB. An individual making a request for a change to or for new</p>	<ul style="list-style-type: none"> • Inquired of the DISA DECC-St. Louis TSB Chief regarding procedures for making changes to system software supporting STANFINS. • Inspected system software change logs to determine whether system software changes on the STANFINS-related mainframe domains were tracked. • Selected a random sample of changes to STANFINS system software/DB changes to determine whether required documentation was present. • Inspected the notification e-mails for STANFINS changes applied during the examination period to determine whether implementation dates for STANFINS were communicated to personnel implementing the changes in the TSB. • Inquired of STANFINS system owners and System Administrators to determine whether procedures were developed and documented for identifying and recording and tracking STANFINS-related system software problems. 	<ul style="list-style-type: none"> • DISA did not develop system software change management procedures detailing specific DECC roles, responsibilities, and procedures regarding identification of system software problems, testing of changes, impact analyses, approvals, implementation and verification, and documentation requirements. • No audit log was created for the use of sensitive system utilities on the ACF2 domains; thus, DISA DECC-St. Louis could not review program use violations. • Top Secret was not consistently configured to generate audit logs for all sensitive utilities; thus, DISA DECC-St. Louis could not review program use violations. • DISA SSO and DISA DECC-St. Louis lacked change documentation that included detailed information about the change, such as test results or impact analysis. • No exceptions noted. • DISA did not develop system software change management procedures detailing specific DECC roles, responsibilities, and procedures regarding identification of system software problems, testing of changes, impact analyses, approvals,

Control Description	Tests of Operating Effectiveness	Results of Tests of Operating Effectiveness
<p>software must submit a request via a Web-based form. The ESCCB board meets on a weekly basis to review the requests submitted over the past week. The policies and procedures of the board set forth the process for submission and approval of change requests.</p> <p>Applicable domains track system software changes.</p>	<ul style="list-style-type: none"> Inspected vendor support agreements to determine whether they were current and provided coverage for computer assets. Inquired of management to determine whether tested and approved STANFINS system software migrated to the production environment was performed by an independent library control group. Compared user listings for individuals with access to migrate changes into the production environment to determine whether it was commensurate with job responsibilities. Inquired of DISA DECC-St. Louis TSB Branch Chief and inspected documentation system-generated inventories to determine whether DISA DECC-St. Louis maintained an inventory of programs on STANFINS-related mainframe domains. 	<p>implementation and verification, and documentation requirements.</p> <ul style="list-style-type: none"> No exceptions noted. The TSB performed the migration of tested and approved system software changes; however, there were no documented policies requiring migration of system software changes into production by an independent library control group. The same person could develop/identify the change request, test the proposed change, and implement the change. At the DECC Mechanicsburg, two individuals listed as authorized users for the Software Factory no longer required access. No exceptions noted.
<p><u>DFAS</u> STANFINS currently operates in a “maintenance mode,” which means that only emergency maintenance changes are applied. Emergency maintenance changes are those software changes required to maintain compliance with applicable Federal statutes and regulations.</p> <p>A completed SCR form must accompany STANFINS software changes with the potential exception of changes required to</p>	<ul style="list-style-type: none"> Inspected supporting authorization and testing documentation for STANFINS changes applied during the examination period to determine whether documentation was prepared in accordance with DoD Instruction 8500.2. 	<ul style="list-style-type: none"> Documentation of testing and authorizations related to the development and implementation of STANFINS application changes were inconsistently generated and maintained. These inconsistencies included: <ul style="list-style-type: none"> SCRs were generally not created if the Change Control Board knew that the request would not be authorized.

Control Description	Tests of Operating Effectiveness	Results of Tests of Operating Effectiveness
<p>accommodate interfacing systems. The System Owner must fill out and approve the SCR before the change is tested and migrated to production.</p> <p>Prior to testing, each SCR requires a documented TCR form to be filled out, including a sign-off documenting the STANFINS PMO Functional group's approval. Testing is performed using production data on a test environment.</p> <p>Once the TCR is authorized, the PMO Functional group sends an e-mail to TSO regarding the change release. A checklist is used to determine that all appropriate steps have been taken prior to ship. DECC is contacted to determine that they are ready to receive, and have received, the release.</p>	<ul style="list-style-type: none"> Performed inquiry of the PMO Accountant and Lead Specialist to verify the process used to document and authorize changes. 	<ul style="list-style-type: none"> Change Control Board meetings were informal, held as needed, and most communication regarding proposed changes was discussed verbally. Of 15 SCRs and TCRs generated October 2, 2002 through October 2004, only three had e-mail documentation to support the change. Of 12 FY 2004 SCRs, only three copies of e-mails notifying the DFAS field sites of changes were maintained. STANFINS application changes were manually controlled, migrated, and released from the testing environment; however, the documentation was not appropriately maintained. Specifically, there was no automated version controls (i.e., a program change version control system) to track changes to STANFINS.
<p>Control Activity: Access controls have been placed into operation to restrict application access to authorized personnel.</p>		
<p><u>DISA</u> The DISA Computing Services Security Handbook details granting access to system resources.</p> <p>Users at the DISA DECC-St. Louis have access to STANFINS application production files and data as necessary to support system operation and respond to customer requests. DECC users also have access to the mainframe GSS where the application resides. The DECC is responsible for creating and maintaining DECC user accounts, as well as DFAS ISSO and TASO accounts at customer sites. The local ISSO/TASO is responsible for creating and maintaining user accounts at customer sites.</p> <p>Users at the DECC (the majority of which are system software</p>	<ul style="list-style-type: none"> Inspected policies and procedures on granting and monitoring access to STANFINS IT resources. Inquired of DISA DECC-St. Louis Security Division Branch Chief to determine the process for granting access to STANFINS. Inspected access control procedures to determine whether the process for granting, monitoring, and removing access to STANFINS followed Federal (NIST SP 800-26 – Logical Access) and DoD guidance (DoD Instruction 8500.2 – Remote 	<ul style="list-style-type: none"> No exceptions noted. No exceptions noted. No exceptions noted.

Control Description	Tests of Operating Effectiveness	Results of Tests of Operating Effectiveness
<p>maintenance personnel) requiring access to the mainframe environment complete a form DD 2875 "System Authorization Access Request", used for initial access requests, as well as for changes to an account. An authorized supervisor must sign this form, indicating approval of the access. Users must possess a security clearance commensurate with the classification level of the system in order to obtain access. Passwords are communicated to users via secure means, either in person or via e-mail, using separate e-mails to transmit user ID and password.</p> <p>The RAS server connections provide direct dial-in access to the network. DECC users requesting remote access must submit an approved form DD 2875. Remote access is granted to users with a valid need, which must be approved by a supervisor, to access the network remotely. Typically, users are granted remote access in order to respond quickly to emergency situations and resolve problems when not at the DECC facility. After receiving an approved remote access request, the Security Division staff adds the user to the RAS server.</p> <p>The mainframe access control applications CA-ACF2 and CA-Top Secret protect the STANFINS application and the system software it resides on.</p> <p>ACF2 and Top Secret mainframe security software enforce discretionary access controls. Also, access to shared and networked file systems outside the mainframe environment is controlled through discretionary access controls enforced through network access privileges.</p> <p>The UML Standardization memo establishes user ID rules for DECC users. DECC user IDs are configured to identify the user's department, as well as employment status. Additionally, the OS/390 STIG requires a unique ACF2 or Top Secret user ID for every user.</p> <p>Passwords are not displayed as a user logs in to the mainframe. After three invalid log-on attempts, ACF2 automatically</p>	<p>Access, Access Procedures, Access Control Policies, Contractor and Foreign Nationals Access, Comprehensive Account Management, Least Privilege Procedures, Classified Data Protection).</p> <ul style="list-style-type: none"> Inspected initial authorization documentation for a random sample of STANFINS users (at the application and network level) to determine completeness and existence. Inquired of DISA DECC-St. Louis Security Division Branch Chief regarding policies and procedures for recertifying users access in STANFINS. Obtained and inspected the ACL for STANFINS to determine whether separated employees had access. Inspected the ACL to determine whether duplicate accounts existed. 	<ul style="list-style-type: none"> At DISA DECC-St. Louis, we selected 42 users out of 1441 and requested their user access request form packets. Out of the sample of 42 packets: <ul style="list-style-type: none"> One user did not have a completed access request form; Three individuals had at least one access request form without a Security representative's signature certifying that the individual's background checks/security clearances were appropriate; Six individuals had at least one access request form where the user acknowledgement portion was not signed. DISA DECC-St. Louis did not have a process for recertifying user access to STANFINS. Two separated out of 11 employees retained access to one or more of the domains where STANFINS resided. No duplicate accounts were identified. (No Exception Noted.) However, three accounts on the Far East domain had no user name associated with the ACF2 ID (ACID). (Exception Noted)

Control Description	Tests of Operating Effectiveness	Results of Tests of Operating Effectiveness
<p>terminates the session. For the Top Secret domains, Top Secret suspends the user's account after two invalid log-on attempts.</p> <p>Before authentication, a warning banner is displayed that informs the user that the system is for authorized use only and that activity will be monitored. The terminal session automatically logs the user off after 15 minutes of inactivity and a screen-lock appears after 15 minutes, which requires the user to re-authenticate in order to re-gain access.</p> <p>Inactive accounts are suspended after 35 days of inactivity and deleted after 90 days of inactivity.</p>	<ul style="list-style-type: none"> Inspected an ACL of remote users and inquired of the ISSO to determine whether the access was limited, documented, and approved. Inquired of Security Division Branch Chief and Security Administrators and inspected ACF2 and Top Secret security settings to determine whether the security products were securely configured in accordance with OS/390 STIG guidance to enforce discretionary access controls. 	<ul style="list-style-type: none"> Remote access to the DECC mainframes via telnet was not restricted and not secured via encryption. Minimum password length on each of the five ACF2 ASIMS domains and the one Top Secret ASIMS domain was configured to six characters, while the OS/390 STIG required passwords have a minimum of eight characters. Users on the Top Secret ASIMS domain were not required by the system to use a national character (e.g., \$, @, #) when creating new passwords, as required by the OS/390 STIG. Users on the ACF2 ASIMS domains were restricted from using their previous four passwords; users should be restricted from using their previous ten passwords as required by the OS/390 STIG. The Huntsville ASIMS domain had the JOBCK setting set to NOJOBCK. This setting did not require ACF2 to verify whether a user submitting a batch job had been granted the authority to submit batch jobs. An individual user was assigned to the Master Central Security Administrator (MSCA) account on the Top Secret ASIMS Far East domain. The MSCA designation allows full system access and is not required for individual users.

Control Description	Tests of Operating Effectiveness	Results of Tests of Operating Effectiveness
	<ul style="list-style-type: none"> Inspected the UML Standardization memo to determine whether naming conventions were established for DECC users. Inquired of Security Division Branch Chief and system administrators to determine security procedures for logging on and using the network. Inspected GSS (mainframe) policies and procedures to determine whether security procedures were documented. Inquired of Security Division Branch Chief and inspected procedures to determine whether inactive mainframe users' accounts were monitored and removed when not needed. Inspected the Top Secret and ACF2 STANFINS-related domain ACLs to determine whether inactive DECC user IDs were present within the domains. Observed an individual user sign on to the mainframe to determine whether the opening screen provided a warning banner 	<ul style="list-style-type: none"> 26 DECC ACF2 accounts on the ASIMS domains had passwords that did not expire (MAXDAYS not specified). 147 DECC Top Secret accounts on the Far East ASIMS domains had passwords that did not expire (Password Interval = 0). DISA DECC St. Louis users had "Write" or "Allocate" access to STANFINS production application datasets on two of five ACF2 ASIMS domains and the Top Secret ASIMS Far East domain. No exceptions noted. No exceptions noted. 542 out of 1392 user accounts across the six STANFINS-related ASIMS domains were inactive for over 180 days or had never been used. No exceptions noted.

Control Description	Tests of Operating Effectiveness	Results of Tests of Operating Effectiveness
	<p>that stated the system was for authorized use only and that activity was monitored.</p> <ul style="list-style-type: none"> Observed a PC terminal to determine whether automatic log-off occurred after a preset number of minutes of inactivity. 	<ul style="list-style-type: none"> No exceptions noted.
<p>DFAS</p> <p>The Procedures for ASIMS Access Controls details policies on security access responsibilities and the process to grant user access to STANFINS. DFAS uses user access forms to document the establishment, modification, deletion, or suspension of access to STANFINS IT resources, to include the STANFINS application, as well as the ELAN, which DFAS administrative and field sites use to gain access to STANFINS.</p> <p>To set up ELAN access, the ELAN administrator, prior to establishing a network user ID and password, must approve the form via signature. For some sites, a separate security group approves the form via signature.</p> <p>Users must have a TAPS account to access the STANFINS application. The local TASO/ISSO is responsible for security administration, including the assignment of TAPS accounts. The ISSO creates user accounts for TAPS/STANFINS through a tool called VASS. For the majority of DFAS field sites, Microsoft Excel spreadsheet, Access database, or other manual means of tracking are used to identify STANFINS/TAPS users, TAPS mode profiles, and assigned TAPS modes. At DFAS-Orlando and DFAS-Japan, TASOs/ISSOs generate ACF2-native listings in order to identify and track access to TAPS and STANFINS.</p> <p>The DFAS ISSP provides guidance in conducting monthly recertifications of STANFINS and ELAN accounts. The ISSO is responsible for providing each supervisor with a STANFINS user listing of access levels, and it is the supervisor's</p>	<ul style="list-style-type: none"> Inspected DFAS policies and procedures to determine whether guidance was established to outline ELAN administrator security responsibilities. Inspected access control procedures to determine whether the process for granting, monitoring, and removing access to STANFINS and GSS followed Federal (NIST SP 800-26 – Logical Access) and DoD guidance (DoD Instruction 8500.2 – Remote Access, Access Procedures, Access Control Policies, Contractor and Foreign Nationals Access, Comprehensive Account Management, Least Privilege Procedures, Classified Data Protection). 	<ul style="list-style-type: none"> Of the four DFAS sites, DFAS-Indianapolis (PMO and TSO), DFAS-Pacific, DFAS-Japan and DFAS-Rome stated that there was no DFAS service-wide policy or guidance document outlining local ELAN administrator security responsibilities versus those of centralized groups responsible for the administration/ monitoring of DFAS-wide network security. During testing, DFAS field sites were unable to generate STANFINS and TAPS user access lists directly from the security system. As a result, of the ten DFAS field sites, DFAS-Rome, DFAS-Denver, DFAS-San Antonio, DFAS-Lawton, DFAS-Columbus, DFAS-Indianapolis and DFAS-Pacific and DFAS-Seaside could not: <ul style="list-style-type: none"> Identify all TAPS modes (access privileges) assigned to users; Determine whether users had inappropriate access to TAPS modes, based on job responsibilities; and Determine whether manually derived and maintained access control lists accurately reflected the user population.

Control Description	Tests of Operating Effectiveness	Results of Tests of Operating Effectiveness
<p>responsibility to validate and authorize user access.</p> <p>Remote network access via a DISP account is granted to a user based on valid need and supervisory approval.</p> <p>STANFINS application password and user ID rules are configured in the security system software maintained by DISA.</p> <p>DFAS ELAN procedures include requirements that guide ELAN administrators in the conduct of network security administration.</p> <p>During log-in to the ELAN, there is a banner warning users that they are about to log on to a government workstation and that their use will be monitored. This banner automatically appears every time a user accesses any DFAS workstation connected to ELAN.</p> <p>ELAN workstations are CAC-configured, which means that an individual must insert a valid CAC card into a reader slot that is connected to the workstation to log in to the network. When the individual leaves the workstation, he or she must remove the CAC card from the reader slot, which automatically locks the workstation and prevents anyone else from accessing it.</p>	<ul style="list-style-type: none"> Inspected access forms for a random sample of STANFINS access (at the application and network level) to determine whether management authorized access. 	<ul style="list-style-type: none"> Of the ten DFAS field sites, nine field sites (DFAS-Rome, DFAS-Denver, DFAS-Lawton, DFAS-San Antonio, DFAS-Columbus, DFAS-Seaside, DFAS-Indianapolis, DFAS-Pacific and DFAS-Japan) either used locally developed or had not documented procedures for granting, approving, monitoring, recertifying, and removing user access to STANFINS and the ELAN. Six of ten DFAS user sites did not have complete or existing authorizations for STANFINS users as follows: <ul style="list-style-type: none"> DFAS-Denver: <ul style="list-style-type: none"> 18 STANFINS user access forms did not have an ELAN Account Request Form on file. DFAS-Pacific: <ul style="list-style-type: none"> Justification for STANFINS user access was pre-populated on user access forms by the TASOs and may not support actual needs. The functional data owner's signature was missing from TAPS user request forms on two of the eight forms inspected. DFAS-Japan: <ul style="list-style-type: none"> Four out of 31 ELAN access request forms that users filled out in 1998 did not have an approval (signature). Two external ELAN users had not signed user agreements. Seven out of 53 DD 2875/DISA 41 forms did not contain a business case for the access request. One out of 53 DD 2875/DISA 41 forms did not contain a business case that

Control Description	Tests of Operating Effectiveness	Results of Tests of Operating Effectiveness
		<p>adequately explained the reasoning for the access request.</p> <ul style="list-style-type: none"> • One out of 26 DISP User Access Request forms could not be found. • Two out of 26 user access forms were not signed by the TASO. • One out of 26 user access forms did not contain a supervisor signature or a business case justification. <p>DFAS-Rome:</p> <ul style="list-style-type: none"> • Three out of 30 user access forms did not have authorization documentation available. • 11 of 29 users with DISP accounts did not have a DISP user access request form with the appropriate approvals and/or justification. Two of these users had STANFINS accounts. <p>DFAS-San Antonio:</p> <ul style="list-style-type: none"> • 32 out of 41 LAN user access forms did not have an access request form on file. <p>DFAS-Seaside:</p> <ul style="list-style-type: none"> • 68 of 72 access request forms did not include an adequate business reason/justification for the access requested. • 46 of 72 access request forms had a pre-populated response that included the type of access the user needed, but did not justify the access. • Three out of 31 internal LAN user access forms did not have the functional data owner's signature. • 14 of 31 internal LAN user access forms did not have the original user access request form used to create their account.

Control Description	Tests of Operating Effectiveness	Results of Tests of Operating Effectiveness
	<ul style="list-style-type: none"> Inquired of DFAS field site ISSOs/TASOs to determine whether DFAS periodically recertified user access levels. Inquired of DFAS ISSOs/TASOs, as well as DFAS field site supervisors, and inspected user access listings to TAPS/STANFINS to determine whether user access was commensurate with job responsibilities. Observed an individual user sign on to the network to note whether the opening screen provided a warning banner that stated the system was for authorized use only and that activity was monitored. 	<ul style="list-style-type: none"> Four of 31 internal users' access request forms were not signed by the information security officer. There was no evidence of LAN access request forms or DISP user access request forms being used prior to February 10, 2005. DFAS field sites did not have the technical knowledge to generate STANFINS and TAPS user access lists directly from the security system. At eight out of ten DFAS field sites (DFAS-Rome, DFAS-Denver, DFAS-Lawton, DFAS-San Antonio, DFAS-Columbus, DFAS-Seaside, DFAS-Indianapolis and DFAS-Pacific), the ISSOs/TASOs could not determine whether manually derived and maintained access control lists accurately reflected the user population, and therefore could not accurately perform user recertifications. At DFAS-Columbus, DFAS-Japan, DFAS-Lawton, DFAS-San Antonio, DFAS-Pacific, DFAS-Rome and DFAS-Seaside, users had access that was not required by their job responsibilities. No exceptions noted.
Control Activity: Integrity verification programs are used by applications to look for evidence of data tampering, errors, and omissions.		
<u>DFAS</u>		

Control Description	Tests of Operating Effectiveness	Results of Tests of Operating Effectiveness
<p>STANFINS uses a batch control method, called “blocking,” to determine whether control totals equal the sum of the details. During the daily production processing cycle, STANFINS performs batch edits for manually entered transactions and transactions received through automated file loads.</p> <p><i>Manual Input</i> Transactions manually entered through TAPS are subject to edits applied to automated transactions submitted for processing during the batch processing cycle.</p> <p><i>Automated File Load</i> Transaction files may also be loaded via FTP. Similar to the TAPS edits, batch edits in STANFINS include the block totals. If a block total is not included in the FTP file, STANFINS will generate a block and then require a user to “accept” the block total in TAPS. The newly generated block will be reported on the Daily Preliminary Balance Report (AVK018).</p> <p>Transaction blocks identified as exceptions by batch edits are suspended and reported on the Daily Preliminary Balance Report (AVK018). Accounting Technicians review the AVK018 and clear erred transactions from the suspense file by submitting a correcting transaction, called a correction card, via TAPS. Items remain in suspense (and on the AVK018) until corrected. Blocks that do pass STANFINS batch edits are reported at a summary level by block in the AVK018.</p>	<ul style="list-style-type: none"> Observed STANFINS batch processing to note whether a block total entered that didn’t match the detailed transactions caused a suspended transaction. Inspected documentation to verify that these suspended transactions were recorded in the AVK018 report. 	<ul style="list-style-type: none"> No exceptions noted.
<p>Control Activity: Reconciliation routines are used by applications, e.g., checksums, hash totals, record counts to promote data accuracy.</p>		
<p><u>DFAS</u> STANFINS uses a batch control method, called “blocking,” to determine whether control totals equal the sum of the details. During the daily production processing cycle, STANFINS performs batch edits for manually entered transactions and transactions received through automated file loads.</p> <p><i>Manual Input</i> Transactions manually entered through TAPS are subject to</p>	<ul style="list-style-type: none"> Observed STANFINS batch processing to note whether a block total entered that didn’t match the detailed transactions caused a suspended transaction. Inspected documentation to verify that these suspended transactions were recorded in the AVK018 report. 	<ul style="list-style-type: none"> No exceptions noted.

Control Description	Tests of Operating Effectiveness	Results of Tests of Operating Effectiveness
<p>edits applied to automated transactions submitted for processing during the batch processing cycle.</p> <p><i>Automated File Load</i></p> <p>Transaction files may also be loaded via FTP. Similar to the TAPS edits, batch edits in STANFINS include the block totals. If a block total is not included in the FTP file, STANFINS will generate a block and then require a user to “accept” the block total in TAPS. The newly generated block will be reported on the Daily Preliminary Balance Report (AVK018).</p> <p>Transaction blocks identified as exceptions by batch edits are suspended and reported on the Daily Preliminary Balance Report (AVK018). Accounting Technicians review the AVK018 and clear erred transactions from the suspense file by submitting a correcting transaction, called a correction card, via TAPS. Items remain in suspense (and on the AVK018) until corrected. Blocks that do pass STANFINS batch edits are reported at a summary level by block in the AVK018.</p>		

Section IV: Supplemental Information Provided by DFAS and DISA

Section IV: Supplemental Information Provided by DFAS and DISA

A. CONTINUITY OF OPERATIONS PLANNING

Continuity of Operations Plan

In a consolidated effort, DFAS and DISA developed a COOP. The COOP possessed the following key characteristics:

- Reflective of current conditions;
- Approved by key affected groups including senior management, Data Center management, and program managers;
- Clearly assigns responsibilities for recovery;
- Includes detailed instructions for restoring operations (both operating systems and critical applications);
- Identifies the alternate processing facility and the backup storage facility;
- Includes procedures to follow when the DECC-St. Louis Data Center is unable to receive or transmit data;
- Identifies critical data files;
- Is detailed enough to be understood by all DFAS system managers;
- Includes computer and telecommunications hardware compatible with the required system needs; and
- Has been distributed to all appropriate personnel.

The COOP provided for backup personnel so that it can be implemented independent of specific individuals. Arrangements were planned for travel and lodging of necessary personnel, if needed. All computer room employees received training on emergency roles and responsibilities. Computer room staff received periodic training in emergency, fire, water, and alarm incident procedures. Emergency response procedures were also documented and periodically tested.

Contracts or interagency support agreements were established for a backup data center and other needed facilities that:

- Were in a state of readiness commensurate with the risk of interrupted operations;
- Had sufficient processing capability; and
- Were likely to be available for use.

Alternate telecommunication services were arranged in the event a disaster rendered the current infrastructure unusable.

The contingency plan was periodically reassessed and, if appropriate, revised to reflect changes in hardware, software, and personnel. The COOP in the STANFINS SSAA was last updated in December 2003. The DISA DECC COOP was updated to include a Lessons Learned section with results of the latest COOP testing in March 2004. Several copies of the contingency plan were securely stored off-site at different locations.

COOP Testing (DISA DECC)

The COOP was tested under conditions that simulated DISA DECC-St. Louis's inability to process critical applications for DFAS. Assumptions were that voice communication, data communication, and public utility services were disabled, the building was not inhabitable, and the processing outage would continue for an extended period of time. DFAS and DISA coordinated efforts to conduct annual disaster recovery tests. Division representatives participated in the tests and were involved in the development of test plans for DFAS systems. Test results were reported to systems managers in writing and the COOP updated to include short- and long-term solutions to problems identified. Additionally, test results were analyzed, and COOP test plans (including test scenarios and test results) were updated after each test. The COOP was also reviewed and updated as necessary.

The most recent disaster recovery test was performed March 8 through March 26, 2004 and included the STANFINS application and underlying GSS. The purpose of the exercise was to test the DECC-St. Louis COOP restoration of all DFAS-Indianapolis and Kansas City critical applications to validate the transfer and processing of data at an alternate location.

The COOP test was successful with the exception of the timeliness of backups. The March 2004 test and full restoration took 124.25 hours versus the 72-hour requirement stated in the STANFINS management and DISA SLA. DISA was taking action to meet the established timeframes.

Acronyms and Abbreviations

ABEND	Abnormal Ending
AC	Access Control
ACF2	Access Control Facility 2
ACL	Access Control Listing
AVK018	Daily Preliminary Balance Report
AVK087	STANFINS General Fund and Inquiry Report
AN	Authorization
APC	Account Processing Code
ASIMS	Army Standard Information Management System
AY	Accuracy
BCL	Block Control Log
C & A	Certification & Accreditation
CAC	Common Access Card
CC	Change Control
CDOIM	Centralized Directorate for Information Management
CICS	Customer Information Control System
COOP	Continuity of Operations Plan/Business Continuity Plan
CP	Completeness
CSOD	Computing Services Operations Division
DARPA	Defense Advanced Research Projects Agency
DARS	Databased Accounting Reconciliation System
DeCA	Defense Commissary Agency
DECC	Defense Enterprise Computing Center
DFAS	Defense Finance and Accounting Service
DISA	Defense Information Systems Agency
DISP	Defense Internet Service Provider
DITSCAP	Defense Information Technology Security Certification and Accreditation Process
DNO	Directorate for Network Operations
ELAN	Enterprise Local Area Network
ESCCB	Executive Software Configuration Control Board
FMFIA	Federal Managers' Financial Integrity Act
FTP	File Transfer Protocol
GSS	General Support System
IA	Information Assurance
IN	Integrity
ISO	Information Services Organization
ISSM	Information Systems Security Manager
ISSO	Information Systems Security Officer
ISSP	Information System Security Plan
IT	Information Technology
LAN	local area network

LPARs	Logical Partitions
MAC	Mission Assurance Category
NIPRNET	non-classified Internet Protocol Router Network
NIST	National Institute of Standards and Technology
NSO	Network Security Officer
NULO	Negative Unliquidated Obligation
OMB	Office of Management and Budget
PIN	Personal Identification Number
PMO	Program Management Office
RACF	Resource Access Control Facility
RAS	Remote Access Service
SAS	Statement on Auditing Standards
SC	Service Continuity
SCR	System Change Request
SP	Security Program
SRR	Security Readiness Review
SS	System Software
SSAA	System Security Authorization Agreement
SSO	System Support Office
STANFINS	Standard Finance System
STIG	Security Technical Implementation Guide
TAPS	Terminal Application Processing System
TASO	Terminal Area Security Officer
TCR	Test Condition Requirements
TSB	Technical Support Branch
TSO	Technical Services Organization

Report Distribution

Office of the Secretary of Defense

Under Secretary of Defense (Comptroller)/Chief Financial Officer
Deputy Chief Financial Officer
Deputy Comptroller (Program/Budget)
Director, Program Analysis and Evaluation

Department of the Army

Inspector General, Department of the Army
Army Audit Agency

Department of the Navy

Auditor General, Department of the Navy

Department of the Air Force

Assistant Secretary of the Air Force (Financial Management and Comptroller)
Auditor General, Department of the Air Force

Combatant Command

Inspector General, U.S. Joint Forces Command

Other Defense Organizations

Defense Finance and Accounting Service
Inspector General, Defense Information Systems Agency

Non-Defense Federal Organizations and Individuals

Office of Management and Budget
Government Accountability Office

Congressional Committees and Subcommittees, Chairman and Ranking Minority Members

Senate Committee on Appropriations
Senate Subcommittee on Defense, Committee on Appropriations
Senate Committee on Armed Services
Senate Committee on Governmental Affairs
House Committee on Appropriations
House Subcommittee on Defense, Committee on Appropriations
House Committee on Armed Services
House Committee on Government Reform

House Subcommittee on Government Efficiency and Financial Management, Committee on Government Reform
House Subcommittee on National Security, Emerging Threats, and International Relations, Committee on Government Reform
House Subcommittee on Technology, Information Policy, Intergovernmental Relations, and the Census, Committee on Government Reform

Team Members

The Defense Financial Auditing Service, in conjunction with contract auditors from KPMG, Bearing Point and the Technical Assessment Division of the Office of Inspector General of the Department of Defense (OIG DoD), prepared this report. Personnel of the Quantitative Methods Division, OIG DoD, also contributed to the report.